Polycom RealPresence Distributed Media Application (DMA) System
Copyright and Trademarks  Copyright© 2020, Plantronics, Inc. All rights reserved. Poly and the propeller design are trademarks of Plantronics, Inc. All other trademarks are property of their respective owners.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street Santa Cruz, California 95060

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Poly Support page for the product.

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

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

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

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

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

Support Visit the Poly Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.
Enable or Disable Automatic Data Collection .............................................. 77
See the Collected Usage Data ................................................................. 77

Signaling Settings .................................................................................. 78
  H.323, SIP, and WebRTC Signaling ..................................................... 78
  SIP and H.323 Gateway ................................................................. 78
  Configuring SIP Settings ................................................................. 79
    Add a SIP Port ............................................................................. 79
    Edit a SIP Port ........................................................................... 80
    Delete a SIP Port ....................................................................... 82
  Configure the SIP Outbound Port Ranges ........................................... 82
    Restore the Default SIP Ports ..................................................... 83
  Configure H.323 Settings ................................................................. 83
  Configure the H.323 Dynamic Port Range ......................................... 84
    Restore the Default H.323 Ports ................................................ 84
  Configure WebRTC Settings .......................................................... 85
  Untrusted SIP Call Handling ............................................................ 85
    Guest Ports ............................................................................... 85
    Dial Rules for Guest Calls .......................................................... 87

High Availability Settings ....................................................................... 90
  Failovers ....................................................................................... 90
  Network Settings to Support High Availability ................................ 91
  High Availability Requirements ..................................................... 92
  Configure High Availability Settings .............................................. 92
    Regenerate a High Availability Encryption Key ........................... 95
  Licensing Calls for High Availability Systems ................................ 96
  Certificates for High Availability Systems ..................................... 96
  Integrating High Availability Systems with the RealPresence Resource Manager System .................................................. 97
  DNS Records for High Availability ................................................. 97

Security Settings ................................................................................. 98
  Selecting a Security Mode .............................................................. 98
    Configure Security Settings ....................................................... 98
    Restrict Security Ciphers .......................................................... 103
    Encryption .................................................................................. 104

Security Certificates ............................................................................ 107
  How Certificates are Used ............................................................. 107
  Accepted Certificates .................................................................... 108
Contents

Edit a Session Profile ................................................................. 186
Delete an MCU ............................................................................. 186
Stop Using an MCU................................................................. 187
Start Using an MCU................................................................. 187
Busy Out an MCU........................................................................ 187
Quarantine an MCU................................................................. 188
Unquarantine an MCU .............................................................. 188
Block Registrations from an MCU............................................. 188
Unblock Registrations from an MCU................................. 188
View Call History ....................................................................... 188

MCU Pools and Pool Orders ..................................................... 190
MCU Selection Process .......................................................... 191
MCU Availability and Reliability Tracking ................................ 192
Working with MCU Pools ....................................................... 193
  View MCU Pools .................................................................. 193
  Add an MCU Pool ............................................................... 193
  Edit an MCU Pool ............................................................... 193
  Delete an MCU Pool ............................................................ 194
Working with MCU Pool Orders ............................................... 194
  Naming Conventions for Pool Orders .................................. 195
  View MCU Pool Orders ...................................................... 195
  Add an MCU Pool Order ..................................................... 195
  Edit an MCU Pool Order ..................................................... 196
  Edit the Priority Ranking of a Pool Order ...................... 196
  Delete an MCU Pool Order .................................................. 197

Integration with Other Services .............................................. 198

Polycom RealPresence DMA System Edge to Core Integration ...... 199
  Run the RealPresence DMA Edge Wizard ............................ 199

Microsoft Active Directory Integration .................................. 201
  Integrate with Active Directory ......................................... 201
  Understanding Base DN ...................................................... 204
  Adding Passcodes for Enterprise Users .............................. 205
    Generate Chairperson and Conference Passcodes for Enterprise Users. 206
  Active Directory Cache Refresh Frequency ....................... 207
  Orphaned Groups and Users ................................................. 207
  About the System's Directory Queries ................................. 209
Configure a Polycom ContentConnect HA Pair for Load Balancing........235
Using Embedded DNS to Share Polycom ContentConnect Systems Across a
Supercluster or HA Pair...................................................................................236
Configure the RealPresence DMA Embedded DNS FQDN in a
Polycom ContentConnect System........................................................236

VPN Tunnel Settings....................................................................................237
Add a VPN Tunnel....................................................................................237
Manually Configure the VPN Tunnel Settings on the Remote
RealPresence DMA System..............................................................................239
Run the RealPresence DMA Edge Wizard on both VPN Tunnel Systems........240
Enable Outbound Calling Through a VPN Tunnel...................................241
Enable Endpoint Provisioning through a VPN Tunnel............................242

Conference Manager Configuration..........................................................244

Conference Settings................................................................................245
Class of Service Overview...........................................................................245
Configure Conference Settings..................................................................245

Conference Templates................................................................-----------249
Standalone Templates...............................................................................249
Templates Linked to Polycom MCU Conference Profiles..........................250

Working with Conference Templates......................................................251
View the Conference Templates List..........................................................251
Add a Standalone Conference Template......................................................251
Add a Linked Conference Template............................................................266
Edit a Conference Template........................................................................267
Delete a Conference Template.....................................................................267

Template Priority.....................................................................................268
Change a Conference Template's Priority................................................268

About Cascading.......................................................................................269
Cascading for Bandwidth...........................................................................269
Processing a Cascaded-for-Bandwidth Call..............................................270
Cascading for Size....................................................................................270
Processing a Cascaded-for-Size Call.......................................................271
Access Control..........................................................................................................................356

Access Control Lists..................................................................................................................357
Access Control List Rules...........................................................................................................357
  View All Access Control List Rules......................................................................................357
  Add an Access Control List Rule.........................................................................................358
  Edit an Access Control List Rule.........................................................................................359
  Copy an Access Control List Rule.......................................................................................359
  Delete an Access Control List Rule......................................................................................360
Access Control List Variables.....................................................................................................360
  Add a Variable.......................................................................................................................360
  Edit a Variable......................................................................................................................361
  Delete a Variable...................................................................................................................362
Access Control List Settings........................................................................................................362
  Add an Access Control List....................................................................................................362
  Edit an Access Control List...................................................................................................363
  Copy an Access Control List..................................................................................................363
  Delete an Access Control List...............................................................................................364
Export Access Control Lists........................................................................................................364
Import Access Control Lists.......................................................................................................364
Add an ACL Rule and Action to an ACL....................................................................................365
Edit an ACL Rule Action for an ACL.......................................................................................365
Delete an ACL Rule from an ACL............................................................................................365
Prioritize ACL Rules in an ACL...............................................................................................366
Disable an ACL Rule in an ACL...............................................................................................366
Enable an ACL Rule in an ACL.................................................................................................366
Assigning ACLs to Ports............................................................................................................366
  Assign an ACL to a SIP Port..................................................................................................367
  Assign an ACL to an H.323 Port..........................................................................................367

Access Proxy Settings................................................................................................................368
Add an HTTPS Proxy..................................................................................................................369
Add a Next Hop..........................................................................................................................371
Edit a Next Hop..........................................................................................................................372
Prioritize Next Hops................................................................................... 372
Delete a Next Hop..................................................................................... 373
Edit an HTTPS Proxy.................................................................................. 373
Add an LDAP Proxy.................................................................................. 374
Edit an LDAP Proxy.................................................................................. 375
Add an XMPP Proxy.................................................................................. 377
Edit an XMPP Proxy.................................................................................. 378
Add a Passthrough Proxy.......................................................................... 379
Edit a Passthrough Proxy.......................................................................... 380
Add an HTTP Tunnel Proxy........................................................................ 381
Edit an HTTP Tunnel Proxy........................................................................ 382
Delete a Proxy.......................................................................................... 382
Configure the Access Proxy Port Range....................................................... 383
Restore the Default Access Proxy Port Range........................................... 384

Media Traversal Settings...................................................................... 385
Configure Media Traversal Settings........................................................... 385
Configure the Media Traversal Port Range................................................ 386
Restore the Default Media Traversal Port Range....................................... 387

TURN Settings....................................................................................... 388
How Allocations Work............................................................................... 388
Configure TURN Settings.......................................................................... 389
TURN Users.............................................................................................. 390
  Add a TURN User.................................................................................. 390
  Edit a TURN User................................................................................ 391
Configure the TURN Port Range................................................................. 391
  Restore the Default TURN Relay Port Range......................................... 392
View TURN Allocations........................................................................... 392

Registration Policies............................................................................. 394
View Registration Policies......................................................................... 395
Registration Policy Scripting.................................................................... 396
  Registration Policy Script Predefined Variables.................................... 396
Add a Registration Policy.......................................................................... 398
  Debug a Registration Policy Script....................................................... 399
Edit a Registration Policy......................................................................... 400
Copy a Registration Policy....................................................................... 400
Delete a Registration Policy..................................................................... 401
Assigning Registration Policies to Ports.................................................... 401
Sample Registration Policy Scripts.......................................................... 402
<table>
<thead>
<tr>
<th>Device Authentication</th>
<th>408</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 Device Authentication</td>
<td>408</td>
</tr>
<tr>
<td>SIP Device Authentication</td>
<td>409</td>
</tr>
<tr>
<td>Inbound Authentication</td>
<td>409</td>
</tr>
<tr>
<td>Shared Outbound Authentication</td>
<td>409</td>
</tr>
<tr>
<td>Add Device Authentication</td>
<td>411</td>
</tr>
<tr>
<td>Edit Device Authentication</td>
<td>411</td>
</tr>
</tbody>
</table>

| Site Topology                                                                          | 413 |

<table>
<thead>
<tr>
<th>Site Topology</th>
<th>414</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Site Topology for Integrated Polycom Systems</td>
<td>415</td>
</tr>
<tr>
<td>Bandwidth Management</td>
<td>415</td>
</tr>
<tr>
<td>Cascade for Bandwidth Conferences</td>
<td>415</td>
</tr>
<tr>
<td>Supercluster Assignments</td>
<td>415</td>
</tr>
<tr>
<td>Configure Site Topology</td>
<td>416</td>
</tr>
<tr>
<td>Embedded DNS</td>
<td>417</td>
</tr>
<tr>
<td>Enable DNS Publishing</td>
<td>418</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Working with Site Topology</th>
<th>420</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>420</td>
</tr>
<tr>
<td>View the Site List</td>
<td>420</td>
</tr>
<tr>
<td>View the Site Information</td>
<td>421</td>
</tr>
<tr>
<td>Add a Site</td>
<td>422</td>
</tr>
<tr>
<td>Edit a Site</td>
<td>428</td>
</tr>
<tr>
<td>Add a Subnet</td>
<td>433</td>
</tr>
<tr>
<td>Edit a Subnet</td>
<td>434</td>
</tr>
<tr>
<td>Network Clouds</td>
<td>434</td>
</tr>
<tr>
<td>View Network Clouds</td>
<td>435</td>
</tr>
<tr>
<td>Add a Network Cloud</td>
<td>435</td>
</tr>
<tr>
<td>Edit a Network Cloud</td>
<td>435</td>
</tr>
<tr>
<td>Site Links</td>
<td>436</td>
</tr>
<tr>
<td>Add a Site Link</td>
<td>436</td>
</tr>
<tr>
<td>Edit a Site Link</td>
<td>437</td>
</tr>
<tr>
<td>Site-to-Site Exclusions</td>
<td>438</td>
</tr>
<tr>
<td>View Site-to-Site Exclusions</td>
<td>438</td>
</tr>
<tr>
<td>Add a Site-to-Site Exclusion</td>
<td>438</td>
</tr>
<tr>
<td>Territories</td>
<td>438</td>
</tr>
<tr>
<td>View the Territories List</td>
<td>439</td>
</tr>
</tbody>
</table>
Licenses............................................................................................................... 580
Networks.............................................................................................................. 581
Server Resources.................................................................................................584
Data Synchronization........................................................................................... 585
System Health and Availability............................................................................. 586
Cluster Features...................................................................................................587
MCUs................................................................................................................... 589
Endpoints............................................................................................................. 592
Conference Manager............................................................................................594
Conference Status................................................................................................594
Skype for Business Presence Publishing.............................................................596
Call Server............................................................................................................599
Call Bandwidth Management................................................................................599

Troubleshooting Utilities................................................................................. 600
Run Network Packet Capture................................................................................600
Run Ping............................................................................................................... 601
Run Traceroute.....................................................................................................601
Run Top................................................................................................................601
Run I/O Stats....................................................................................................... 602
Run SAR.............................................................................................................. 602
Check NTP Status................................................................................................. 602
Manually Synchronize all Clusters........................................................................ 602
Reset to Default Settings...................................................................................... 603
Diagnostics for your Polycom Server................................................................... 604

RealPresence DMA System Network Configurations............................... 605
Legend................................................................................................................. 605
Core Configurations............................................................................................. 606
Single Core System to Edge System................................................................. 606
Active-Passive HA Core Systems to Edge System.......................................... 606
Active-Active HA Core Systems to Edge System............................................ 607
Supercluster with Single Core System to Edge System.................................... 607
Supercluster with Active-Passive HA Core Systems to Edge System............. 608
Edge Configurations........................................................................................... 608
Single Edge System to Core System................................................................. 608
Active-Passive HA Edge Pair to Core System.................................................. 609
Active-Active HA Edge Pair to Core System.................................................... 609
VPN Tunnel Between Edge System and Combination System....................... 610
VPN Tunnel Between Two Edge Systems Communicating with Core System.... 610
Combination Configurations................................................................. 611
Edge System, No Core System............................................................... 611
Active-Passive HA Edge Pair, No Core System................................. 612
Active-Active HA Edge Pair, No Core System................................. 612
Before You Begin

Topics:

- Audience, Purpose, and Required Skills
- Related Poly and Partner Resources

The Polycom RealPresence Distributed Media Application (DMA) Administrator Guide provides instructions to configure and administer your RealPresence DMA system.

Audience, Purpose, and Required Skills

The primary audience for this guide is system administrators and network engineers who configure, maintain, and support the telecommunications infrastructure and video conferencing environment.

To perform some of the implementation and maintenance tasks described in this guide, the administrator should have basic technical knowledge and skills in the following disciplines:

- Current telecommunications practices, protocols, and principles
- Telecommunication basics and video teleconferencing
- Networking, security certificates, and software configuration

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Polycom Support Site is the entry point to online product, service, and solution support information including Licensing & Product Registration, Self-Service, Account Management, Product-Related Legal Notices, and Documents & Software downloads.
- The Polycom Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Polycom Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The Polycom Partner Network are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers’ current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The Polycom Collaboration Services help your business succeed and get the most out of your investment through the benefits of collaboration.
Getting Started

Topics:

- RealPresence DMA System Overview
- Working in the RealPresence DMA System
- DNS Records for the RealPresence DMA System

The following topics provide an introduction to the Polycom RealPresence DMA system features and initial configuration.
The RealPresence DMA system is a reliable and scalable video collaboration infrastructure solution. The following topics introduce you to the system:

### Core and Edge Configuration Options

The RealPresence DMA system supports two types of configuration: core configuration and edge configuration.

When you deploy one or more RealPresence DMA systems, you need to set up each system with a core configuration, an edge configuration, or a combination configuration as follows:

- A core configuration if you deploy the system inside your enterprise network environment.
- An edge configuration if you deploy the system in the DMZ and it communicates with one or more core-configured systems inside your enterprise network.
- A combination configuration if the system is one of the following:
  - An edge-configured system that resides in the DMZ and doesn’t communicate with any core configured system. The system can handle registrations, calls, firewall/NAT traversal, and conferences with virtual meeting rooms.
  - An edge-configured system inside the enterprise that is part of a VPN tunnel and doesn’t communicate with any core configured system. The system can handle registrations, calls, and conferences with virtual meeting rooms.

See the Polycom RealPresence DMA System Getting Started Guide for installation instructions.

### Polycom RealPresence DMA System Supported Features

The RealPresence DMA system provides all features in an edge, core, or combination configuration. Therefore, specific systems can be configured in a variety of ways, but not all configurations are supported.

The following table lists the tested and supported features and configurations:

<table>
<thead>
<tr>
<th>Feature/Configuration</th>
<th>Edge System</th>
<th>Core System</th>
<th>Combination System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access proxy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature/Configuration</td>
<td>Edge System</td>
<td>Core System</td>
<td>Combination System</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Access Control Lists</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Directory integration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clariti VMR licensing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conference management (MCUs, VMRs, conference templates, conference settings)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge services</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded DNS</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>External H.323 gatekeepers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External SIP peers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>H.323</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>High Availability (HA)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>High Availability support for Polycom ContentConnect HA and geo-redundancy</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Immersive Telepresence (ITP) layout</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IVR</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MCU conference thresholds</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Media traversal (relay)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NAT</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Polycom ContentConnect (PCC) integration</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature/Configuration</td>
<td>Edge System</td>
<td>Core System</td>
<td>Combination System</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>RealPresence Resource Manager integration (site topology, scheduling)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RealPresence Resource Manager licensing (Clariti)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Registration sharing (from)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REST API</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security settings</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Shared number dialing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SIP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SIP conference factories</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Site topology</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Skype for Business integration</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Superclustering</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Synchronize pooled conference name from the RealPresence Resource Manager system to RMX</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TIP version 8 support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TURN</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN tunnel</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WebRTC</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Unsupported Configurations**

The following configurations of one or more RealPresence DMA systems are not supported.

Note that the use of unsupported features and configurations will not be prevented.

- Superclustering of systems in edge configuration
- Superclustering of systems in edge standalone configuration (combination systems)
- Superclustering between systems in edge configuration and systems in core configuration
The RealPresence DMA System's Primary Functions

The RealPresence DMA system provides the following primary functions:

- Conference manager
- Call server
- Firewall/NAT traversal
- RealPresence Platform API
- SVC conferencing support

Conference Manager

The Polycom RealPresence DMA system's conference manager facilitates multipoint video conferencing. A multipoint video conference is one in which multiple endpoints are connected, with all participants able to see, and hear each other. The endpoints connect to a media server (MCU), which processes the audio and video from each and sends the conference audio and video streams back to them.

Traditionally, such multipoint conferences had to be scheduled in advance, reserving ports on a specific MCU, in order to ensure the availability of resources. The conference manager makes this unnecessary. The conference manager uses advanced routing policies to distribute voice and video calls among multiple MCUs, creating a single virtual resource pool. This greatly simplifies multipoint video conferencing resource management and uses MCU resources more efficiently.

The RealPresence DMA system integrates with your Microsoft Active Directory, automating the task of provisioning users with virtual meeting rooms (VMRs), which are available for use at any time for multipoint video conferencing. Combined with its advanced resource management, this makes reservationless (ad hoc) video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.

The RealPresence DMA system's ability to handle multiple MCUs as a single resource pool makes multipoint conferencing services highly scalable. You can add MCUs on the fly without impacting end users and without requiring reprovisioning. The RealPresence DMA system can span a conference across two or more MCUs (called cascading), enabling the conference to contain more participants than any single MCU can accommodate.

The conference manager continually monitors the resources used and available on each MCU and intelligently distributes conferences among them. If an MCU fails, loses its connection to the system, or is taken out of service, the RealPresence DMA system distributes new conferences to the remaining MCUs. Every conference on the failed MCU is restarted on another MCU (provided there is space available). The consequences for existing calls in those conferences depend on whether they're H.323 or SIP:

- H.323 participants are not automatically reconnected to the conference. In order to rejoin the conference, dial-in participants simply need to redial the same number they used for their initial dial-in. Dial-out participants will need to be dialed out to again; the RealPresence DMA system doesn't automatically redial out to them.
- SIP participants are automatically reconnected to the conference on the new MCU. This includes both dial-in and dial-out SIP participants. No new dial-out is needed because the RealPresence
DMA system maintains the SIP call leg to the participant and only has to re-establish the SIP call leg from the RealPresence DMA system to the MCU.

Call Server

The RealPresence DMA system's call server provides the following functionality:

- H.323 gatekeeper
- SIP registrar and proxy server
- H.323 <-> SIP transition gateway
- Dial plan and prefix services
- Device authentication
- Bandwidth management

Firewall/NAT Traversal

The RealPresence DMA system enables users within and beyond your firewall to securely access voice, video, and multimedia sessions across IP network borders.

The system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP, H.323, and WebRTC video calls (including H.460 firewall/NAT traversal) from registered users, guests, and federated enterprises or divisions.

RealPresence Platform API

The RealPresence DMA system optionally allows an API client application, developed by you or a third party, to access the Polycom RealPresence Platform Application Programming Interface (API).

The API provides programmatic access to the RealPresence DMA system for the following:

- Provisioning
- Conference control and monitoring
- Call control and dial-out
- Billing and usage data retrieval
- Resource availability queries

The API uses XML or JSON encoding over HTTPS transport and adheres to a Representational State Transfer (REST) architecture.

**Note:** The API communicates asynchronously. Clients subscribing to event notifications via the API must be prepared to receive notifications out of order.

A RealPresence Resource Manager system can integrate with the RealPresence DMA system via the API. The API provides the full programmatic access to the RealPresence DMA system described above and enables users of the RealPresence Resource Manager scheduling interface to:

- Schedule conferences using the RealPresence DMA system's MCU resources.
- Set up *Anytime* conferences. Anytime conferences are referred to as *preset dial-out* conferences in the RealPresence DMA system.
SVC Conferencing Support

The RealPresence DMA system supports the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC), for both point-to-point and multipoint (VMR) calls.

SVC is sometimes referred to as layered media because the video streams consist of a base layer that encodes the lowest available quality representation plus one or more enhancement layers that each provide an additional quality improvement. SVC supports three dimensions of scalability: temporal (frames per second), spatial (resolution and aspect ratio), and quality (signal-to-noise ratio).

The video stream to a device can be tailored to fit the bandwidth available and device capabilities by adjusting the number of enhancement layers sent to the device.

For multipoint conferencing, the MCU doesn't have to do processing-intensive mixing and transcoding to optimize the experience for each device. Instead, it simply passes the video stream from each device to each device, including the enhancement layers that provide the best quality the device can support.

Polycom's SVC solution focuses on the temporal and spatial dimensions. It offers a number of advantages over standard AVC conferencing, including:

- Improved video quality at lower bandwidths
- Improved audio and video error resiliency (good audio quality with more than 50% packet loss, good video quality with more than 25% packet loss)
- Lower end-to-end latency (typically less than half that of AVC)
- More efficient use of bandwidth
- Lower infrastructure cost and operational expenses
- Easier to provision, control, and monitor
- Better security (end-to-end encryption)

Polycom's SVC solution is supported by the Polycom RealPresence Platform and Environments, including the latest generation of Polycom MCUs and RealPresence room, personal, desktop, and mobile endpoints. Existing RMX MCUs with MPMx cards can be made SVC-capable with a software upgrade, and doing so triples their HD multipoint conferencing capacity.

RealPresence Collaboration Server 800s MCUs support mixed-mode (SVC+AVC) conferences. Both SVC and AVC endpoints can join the conference, and each gets the appropriate experience: SVC endpoints get SVC mode and get a video stream for each AVC participant; AVC endpoints get a single Continuous Presence (CP) video stream of the participants (both AVC and SVC) supplied by the MCU.

When the RealPresence DMA system selects an MCU that doesn't support SVC for a conference configured for mixed mode, it starts the conference as an AVC-only conference (all SVC-capable endpoints also support AVC). But if the MCU supports SVC but not mixed mode (RMX 7.8), the conference fails to start.

Refer to your RealPresence Collaboration Server or RMX documentation for important information about the MCU's implementation of SVC conferencing and its configuration, limitations, and constraints.
The RealPresence DMA System's Three Configurations

Depending on your organization's needs, you can deploy the RealPresence DMA system in one of the following three configurations.

Two-server Configuration

Two core-configured or two edge-configured RealPresence DMA systems can be set up on the same network to provide high availability (HA) of services.

Systems configured for HA support minimal interruption of services and greater call reliability.

The RealPresence DMA system supports two HA configurations:

- **Active-passive** - The two RealPresence DMA systems share one set of virtual IP addresses for each enabled network interface with services assigned. If one system fails, the peer system takes over the failed system's resources (virtual IP addresses and assigned services). All active calls are either dropped automatically or callers must manually hang up, but registration and provisioning information for endpoints is maintained in memory and shared between both systems. Once all resources are re-established on the peer system, users can call back in to the video conference without changing any call information.

- **Active-active** - Each Real Presence DMA system has virtual IP addresses for each enabled network interface with services assigned. Both systems run concurrently and load balancing occurs between the two systems. This configuration increases throughput for media, making use of both systems so you have full capacity.

  **Note:** An active-active HA pair cannot be part of a supercluster.

Single-server Configuration

The RealPresence DMA system can also be deployed in a single-server configuration.

This configuration offers all the advantages of the RealPresence DMA system except the redundancy and fault tolerance. It can be upgraded to a two-server cluster at any time.

The RealPresence DMA System Operations Guide and online help generally assume a redundant two-server cluster. Where there are significant differences between the two configurations, those are spelled out.

Supercluster Configuration

To provide geographic redundancy and better network traffic management, up to 10 geographically distributed RealPresence DMA system clusters (two-server or single-server) can be integrated into a supercluster.

All five clusters can be call servers (function as gatekeeper, SIP proxy, SIP registrar, and gateway). Up to three can be designated as conference managers (manage an MCU resource pool to host conference rooms).

The superclustered RealPresence DMA systems can be centrally administered and share a common data store. Each cluster maintains a local copy of the data store, and changes are replicated to all the clusters.
Most system configuration is supercluster-wide. The exceptions are cluster-specific or server-specific items like network settings and time settings.

**Clusters versus Superclusters**

Technically, a standalone RealPresence DMA system (two-server or single-server) is a supercluster that contains one cluster.

All the system configuration and other data that are shared across a supercluster are kept in the same data store. At any time, another RealPresence DMA system can be integrated with it to create a two-cluster supercluster that shares its data store.

It’s important to understand the difference between two co-located servers forming a single RealPresence DMA system (cluster) and two geographically distributed RealPresence DMA system clusters (single-server or two-server) joined into a supercluster.

A single two-server cluster has the following characteristics:

- A single shared virtual IP address and FQDN, which switches from one server to the other when necessary to provide local redundancy and fault tolerance.
- A single management interface and set of local settings.
- Ability to manage a single territory, with no territory management backup.
- A single set of call server and conference manager responsibilities.

A supercluster consisting of two clusters (single-server or two-server) has the following characteristics:

- Separate IP addresses and FQDNs for each cluster.
- Separate management interfaces and sets of local settings for each cluster.
- Ability for each cluster to manage its own territory, with another cluster able to serve as backup for that territory.
- Different call server and conference manager responsibilities for each territory and thus each cluster.
Working in the RealPresence DMA System

Topics:

▪ Accessing the System
▪ Navigating the System
▪ Customize Your Dashboard
▪ View System Alerts
▪ Refreshing Data
▪ Field Input Requirements
▪ Sorting Data by Columns
▪ Web Browsers
▪ Ports Summary

You can configure and manage the RealPresence DMA system by using the management user interface. Its Dashboard and menus provide access to call server and conference manager functions. The topics in this section include general information you need to work in the RealPresence DMA system.

Accessing the System

When you log in to the RealPresence DMA system, the system Dashboard displays.

Log In to the System

You need to log in to the management user interface from a client system with a browser that supports HTML5.

Note: Most browsers provide options to save login credentials for applications or websites you access. Browsers may also "auto-complete" field information you have previously entered, including user names and passwords. To increase the security of your RealPresence DMA system, Polycom recommends that you disable any saved credentials or auto-complete options in your browser settings.

Procedure

1. Point your browser to the host name or IP address of your system.
2. Enter your username and password and click Log in.

The RealPresence DMA system dashboard displays.

Sign Out of the System

You can sign out of the RealPresence DMA system from the dashboard.
Procedure

» Click admin and select Sign Out.

**Change Your Password**

You can configure the system to expire local user passwords after a certain number of days.

If your password has expired, the system prompts you for a new password when you try to sign in to the management user interface.

You can change your password at other times, as needed.

**Procedure**

1. Click admin and select Change Password.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user name with which you're logging in. Display only.</td>
</tr>
<tr>
<td>Old password</td>
<td>For security reasons, you must re-enter your old password.</td>
</tr>
<tr>
<td>New password</td>
<td>Enter a new password. The password must satisfy the local password rules specified for the system.</td>
</tr>
<tr>
<td>Confirm new password</td>
<td>Retype the password to confirm that you entered it correctly.</td>
</tr>
</tbody>
</table>
3. Click OK.

**Navigating the System**

You can use the system **Dashboard** to view information about system health and activity levels.

The Dashboard panes provide details about numerous RealPresence DMA system functions. You can open more than one instance of any pane.

To return to the **Dashboard** from any other page, click the Polycom logo to the left of the menus.

**Active Directory Integration Pane**

Displays information about the status of Active Directory integration.

If the system is integrated with AD, this pane shows:

- The territory (and cluster) responsible for refreshing the cache.
- When the cache was last refreshed and by which server.
- The AD server address and user ID used.
- The number of enterprise conference rooms created.

The **Link** button takes you to the Microsoft Active Directory page.
Call Server Active Calls Pane
Displays the total number of active calls on all RealPresence DMA systems, the total number on each system, the total number of active calls of each signaling type, the total licensed call limit for all systems, and the total licensed call limit for each system.

If H.323 signaling is enabled, the call mode (direct or routed) also displays.

The Call Server Active Calls pane only displays counts of calls that consume a license from the local RealPresence DMA system. You can view all active calls on the RealPresence DMA system from Monitoring > Active Calls or Reports > Call History.

Examples:
▪ If your RealPresence DMA edge system is unlicensed and an endpoint registered to the edge system calls a VMR that's hosted on the core system, the call isn’t counted on the Call Server Active Calls pane of the edge system. Note that the edge system is configured as a SIP peer or neighbored gatekeeper of the core system where the license is consumed.
▪ If your edge system is unlicensed and an endpoint registered to the edge system makes a point-to-point call to another endpoint registered to an edge system or to anyone on the internet (including a Video as a Service (VaaS) conference), the call is counted on the Call Server Active Calls pane of the edge system. Note that the edge system consumes a license from the core system using the license sharing feature.
▪ If your edge system is unlicensed and an endpoint registered to the core system makes an outbound internet call through the edge system, the call is counted on the Call Server Active Calls pane of the edge system. Note that the edge system consumes a license from the core system using the license sharing feature.

The Link button on the pane takes you to the Active Calls page.

Call Server Registrations Pane
Displays the total number of active (including active quarantined) and inactive (including inactive quarantined and blocked) endpoint registrations and the number that failed in the past 24 hours.

Hover over a registration number to see the limit.

Also displays the total number of registrations for each cluster of the supercluster. Hover over a cluster's total to see the breakdown between active and inactive.

The Link button takes you to the Endpoints page.

Cluster Information Pane
Displays detailed information about the selected cluster.

For a two-server cluster, the pane contains a tab for each server. The tab label indicates which server is currently active. Each tab contains the following information about the server:
▪ Current date, time, and uptime
▪ System version number
▪ Hardware model and serial number
▪ Time source
▪ Management network MAC and physical and virtual IPv4 and IPv6 addresses
▪ Signaling network MAC and physical and virtual IPv4 and IPv6 addresses
▪ CPU utilization percentage (all cores)
- System memory usage (it's normal for memory usage to be high)
- Swap space (total and free)
- Disk space usage (actual and percentage)
- Log space usage (actual and percentage) and next scheduled log purge

**Conference History - Max Participants Pane**

Displays a bar graph showing variations in the maximum number of conference manager conference participants over the time span you select.

The graph shows the data for all conference manager clusters. The *Ad hoc participants* category includes all dial-outs and all dial-ins to non-scheduled conferences. The *Other participants* category includes all dial-ins to conferences scheduled via Polycom Conferencing for Outlook (calendared conferences) or via an API client such as the RealPresence Resource Manager system.

The **Link** button takes you to the Conference History page.

**Conference Manager MCUs Pane**

Displays information about all MCUs that are managed by the conference manager to host conference rooms (virtual meeting rooms, or VMRs).

The information shown includes the MCU's connection and service status, its capabilities, its reliability (disconnects and call failures), and the number of ports in use and available to the conference manager.

The **Link** button takes you to the **MCUs** page.

**Note:** An MCU may be connected to up to three conference manager clusters. If one of the three conference managers loses its connection to the MCU, this is counted as 0.33 disconnects. If all connections to the MCU are lost, this is counted as 1 disconnect.

**Conference Manager Usage Pane**

Displays usage information for the conference manager, either for all conference manager clusters or for the selected cluster.

The information shown includes the territories for which conference manager is enabled, the number of conferences and participants, the port usage, and the number of local users and custom conference rooms.

**Note:** The RealPresence DMA system reports port numbers based on CIF resource usage. Version 8.1 and later Polycom MCUs report HD720p30 port numbers. In general, 3 CIF = 1 HD720p30, but it varies depending on bridge/card type and other factors. See your Polycom RMX or RealPresence Collaboration Server documentation for more detailed information about resource usage.

**Exchange Server Integration Pane**

If the RealPresence DMA system is integrated with a Microsoft Exchange server, the pane displays the following:

- The server in the cluster performing Exchange server integration and integration status, which can be one of the following:
Unavailable - A service status or inter-server communication problem prevented determination of the integration status.

Error - The system was unable to establish a connection to the Exchange server. This could be a network or Exchange server problem, or it could be a login failure.

Awaiting Active Directory - The system isn't integrated with the Active Directory, required for Exchange server integration.

Primary SMTP mailbox not found - The mailbox configured for the RealPresence DMA system isn't in the system's Active Directory cache.

Subscription pending - The RealPresence DMA system has asked the Exchange server to send it notifications and is waiting to receive its first notification to confirm that the Exchange server can communicate with the system. If this status persists for more than a minute or so, there is likely a configuration problem (such as an invalid certificate or the Exchange server is unable to resolve the RealPresence DMA system's FQDN).

Exchange authentication failed - The credentials for the RealPresence DMA system's mailbox are no longer valid (for example, the password has expired).

OK - The RealPresence DMA system is receiving and processing Polycom Conferencing meeting notifications from the Exchange server.

- The territory configured for Exchange server integration, color-coded according to supercluster status.
- The host name or IP address for the Exchange server as entered on the Microsoft Exchange Server page.
- The RealPresence DMA system's mailbox address.
- The number of Polycom Conferencing meetings today.

The Link button takes you to the Microsoft Exchange Server page.

High Availability Status Pane

If two RealPresence DMA systems are configured in High Availability (HA) mode, the pane displays the following:

- Local physical IP address of the interface that is assigned the management service, HA connection status, VIP owner status.
- Peer physical IP address of the interface that is assigned the management service, HA connection status, VIP owner status.
- Status of each network interface enabled as an HA link or that has a virtual IP address (Up or Down).
- Virtual IP address for the interface (if services are assigned to it).
- Whether the HA network interfaces are connected (peer-to-peer) via crossover cable.

Licensed Virtual Meeting Rooms Pane

If a RealPresence DMA system is licensed for concurrent Virtual Meeting Rooms (VMRs), the pane displays counts of active VMRs and licensed VMRs.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Active</td>
<td>Shows the number of active VMRs on the following:</td>
</tr>
<tr>
<td></td>
<td>▪ Single system</td>
</tr>
<tr>
<td></td>
<td>▪ Active system in an active-passive HA pair</td>
</tr>
<tr>
<td></td>
<td>▪ Both systems in an HA active-active pair</td>
</tr>
<tr>
<td>Local Licensed</td>
<td>Shows the total number of VMR licenses on the following:</td>
</tr>
<tr>
<td></td>
<td>▪ Single system</td>
</tr>
<tr>
<td></td>
<td>▪ Both systems in an HA active-passive pair</td>
</tr>
<tr>
<td></td>
<td>▪ Both systems in an HA active-active pair</td>
</tr>
<tr>
<td>Supercluster Active</td>
<td>Shows the number of active VMRs on all systems in the supercluster.</td>
</tr>
<tr>
<td>Supercluster Licensed</td>
<td>Shows the total number of VMR licenses on all systems in the supercluster.</td>
</tr>
</tbody>
</table>

**RealPresence Resource Manager System Integration Pane**

If the RealPresence DMA system is integrated with a RealPresence Resource Manager system, displays the following:

- Host name or IP address of the RealPresence Resource Manager system.
- User name used to log into the RealPresence Resource Manager system.
- Time when site topology data was last updated from the RealPresence Resource Manager system.
- Number of territories, sites, site links, and network (MPLS) clouds in the site topology data obtained from the RealPresence Resource Manager system.

The **Link** button takes you to the [RealPresence Resource Manager](#) page.

**Server Interfaces Pane**

Displays the network interfaces for the server and the services, if any, that are assigned to each interface.

**Signaling Settings Pane**

Displays the H.323, SIP, and WebRTC signaling settings for the selected cluster, including whether each protocol is enabled and what ports are assigned.

**Supercluster Status Pane**

Displays the status of each server in every cluster of the supercluster, the status of its private, management, and signaling interfaces, and the territory for which it's responsible.

A territory is green if being managed by its primary cluster, yellow if being managed by its backup cluster, and red if it's out of service (no cluster is managing it). Hover over a name or icon to see more details.

The icons in the Status column indicate the status of the server. Hover over an icon to see further details.

The **Link** button takes you to the [DMAs](#) page.
**Territory Status Pane**

Lists each territory, its capabilities, and the primary and backup cluster responsible for it.

You can hover over the text and icons to see more details. The territories are color-coded, each color with its own tool tips:

- **Green**: Active on primary cluster - The primary cluster for the territory is in service. The backup cluster may or may not be assigned.
- **Yellow**: Indicates one of the following:
  - Active on primary cluster - The primary cluster for the territory is unreachable from some clusters including the backup cluster. The backup cluster is not in service or is not assigned.
  - Active on backup cluster - The primary cluster for the territory is not in service or not assigned, but the backup cluster is in service.
  - Active on both primary and backup clusters - The primary cluster for the territory is unreachable from some clusters including the backup cluster, and the backup cluster is in service. The ownership of the territory is split between the primary and backup clusters.
- **Red**: Indicates one of the following:
  - Not active; associated clusters not in service - A primary or backup cluster is assigned to the territory (or both), but neither the primary nor the backup cluster are in service.
  - Not active; no primary or backup cluster assigned - No clusters are assigned to the territory.

Note that a cluster is considered in service if it is reachable from the backup cluster, even if it is unreachable from some of the other clusters. A cluster is considered not in service if it has been given the Stop Using command, is busied out, or is unreachable.

The Link button takes you to the Territories page.

**TURN Status Pane**

Shows the TURN server status.

**Running** displays in green, **Stopped** displays in red. The pane also shows the total number of TURN allocations and the total TURN bandwidth in kbps.

**User Login History Pane**

Displays the following information about logins by your user ID:

- The server you’re currently logged in to.
- The time, date, server logged in to, and source (host name or IP address) of the last successful login (prior to your current session) by your user ID.
- The time, date, server, and source of the last failed login attempt by your user ID.
- The number of consecutive failures before your current successful login.
Customize Your Dashboard

You can customize your Dashboard to display panes that contain information about various system functions.

Initially, the Dashboard contains six default panes. You can add other panes or close any that you don’t want to view. You can also add multiple copies of the same pane, with each showing information for a different cluster. The maximum number of panes is 50.

The buttons on the right side of each pane’s title bar let you access help, go to a related page (where appropriate), maximize the pane to fill the window, restore it to its normal size, or close the pane. Hover over a button to see what it does.

Note that the RealPresence DMA system stores your Dashboard layout in your web browser’s cache. If you log in to the system from different devices, your Dashboard view may differ.

Procedure

1. Click Edit to enable the Dashboard editing options.
2. Select from the following:
   - Add - displays a list of panes you can add to the Dashboard.
   - Save - saves your changes to the Dashboard.
   - Auto-arrange - arranges the panes to best fit your browser window.
   - Restore Defaults - restores the Dashboard to the six default panes.
   - Cancel - cancels your changes.

View System Alerts

An alert icon appears in the main menu bar and displays the number of alerts, if any, currently affecting the system.

Procedure

1. Click to display the current alerts.
2. Click on an alert link to display the area of the system affected by the alert.

Refreshing Data

Data within the RealPresence DMA system can be automatically refreshed on some pages in the management user interface and manually refreshed on all pages in the management user interface.

Set the Automatic Refresh Rate

Automatically refreshing the data on a page within the management user interface updates the data that display at an interval you define.

You can set an automatic refresh rate of 5, 15, 30, 45 seconds, or 1 minute. When the RealPresence DMA system refreshes data, it takes several seconds to collect the data and deliver it to the management user interface. The system collects data as quickly as possible, but if you set the refresh rate to 5 seconds, the data returned are not guaranteed to be 5 seconds old at the most.
Note that when you select a refresh rate on a given management user interface page, the rate will apply to all pages that have the automatic refresh feature. The rate will also persist for future logins if the same user logs in from the same computer, using the same web browser.

**Procedure**

1. Go to any RealPresence DMA system management user interface page that has the automatic refresh icon (○).
2. Select **Settings** next to the automatic refresh icon and choose a refresh rate.
   The data on the page will automatically refresh at the rate you selected.

**Refresh Data Manually**

You can manually refresh the data on a management user interface page at any time by clicking the manual or automatic refresh icon.

**Procedure**

» Go to any RealPresence DMA system management user interface page that has the manual refresh icon (○) or automatic refresh icon (○) and click the icon.
   The data on the page will refresh.

**Field Input Requirements**

While every effort was made to internationalize the RealPresence DMA system, not all system fields accept Unicode entries.

If you work in a language other than English, be aware that some fields accept only ASCII characters.

For input fields that accept a SIP URI, the supported characters for the `userinfo` portion of the URI include:

- **Alpha**: a-z, A-Z
- **Numeric**: 0-9
- **Escaped**: %XX where X=0-9, A-F, a-f
- **Other**: -_!!*'(;)::=+$,

For input fields that accept an H.323 alias, the supported characters include:

- All ASCII characters in the ranges %x21-24,%x26-3F,%x41-7f
- % @ and values < %x21 can be escaped.
- **Escaped**: %XX where X=0-9, A-F, a-f

**Sorting Data by Columns**

The RealPresence DMA system management user interface often displays data, for example, search results, in a table (grid) format.

If the data is more than one page, each page displays 100 results. You can sort data by clicking a column header; however, the system will sort only the current page. If you’ve more than one page of results, you need to sort by column on each page.
Web Browsers

When you access the management user interface, the browser you use stores the web page information in a temporary cache memory file.

When you make certain changes to the RealPresence DMA system that cause a system restart or that alter a security certificate, you may need to refresh or reload your browser to update the management user interface before you log back in. You may also need to refresh your browser if you receive system errors while downloading log files.

If you refresh your browser and still see outdated information or can't download log files in the RealPresence DMA system, you need to clear your browser's cache. See the instructions for your specific browser.

Ports Summary

The following table lists the default port settings used by RealPresence DMA for communication with other devices (you can also find this information in the Poly RealPresence DMA System Administrator Guide).

ICMP (ping) is useful between all private network devices and for public network diagnostics. If you have RealPresence Resource Manager managing RealPresence DMA, then you must enable ICMP between the two servers.

Note that this table is intended as general guidance, and ports may vary depending on specific configurations and/or services used.

### RealPresence DMA System Inbound and Outbound Ports

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>RealPresence DMA Configuration</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Public IP</td>
<td>Any</td>
<td>Access proxy services-public interface IP</td>
<td>389, 443, 5222, 9950 – 9999</td>
<td>TCP/UDP (either or both)</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Access proxy services-public</td>
<td>Access proxy ports depending on configured instances</td>
</tr>
<tr>
<td>Access proxy services-private interface IP</td>
<td>10000 – 13000</td>
<td>Any Private IP</td>
<td>Any</td>
<td>TCP/UDP (either or both)</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Access proxy services-private</td>
<td>Access proxy dynamic ports</td>
</tr>
<tr>
<td>Access proxy services-private interface IP</td>
<td>&gt;1023</td>
<td>RealPresence Resource Manager</td>
<td>389, 443, 5222</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Access proxy services-private</td>
<td>Access proxy (private) communication with RealPresence Resource Manager</td>
</tr>
<tr>
<td>Access proxy services-private interface IP</td>
<td>&gt;1023</td>
<td>RealPresence Web Suite</td>
<td>443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Access proxy services-private</td>
<td>Access proxy (private) communication with RealPresence Web Suite</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination IP</td>
<td>Destination Port</td>
<td>Protocol</td>
<td>Direction</td>
<td>RealPresence DMA Configuration</td>
<td>Interface</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
<td>---------------------------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------------------------</td>
<td>-----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Media traversal services private interface IP</td>
<td>40002 – 50998</td>
<td>TCP/UDP</td>
<td>Inbound</td>
<td>Media traversal services-private</td>
<td>Edge or Combo</td>
<td>Media traversal (private)</td>
</tr>
<tr>
<td>Media traversal services private interface IP</td>
<td>40002 – 50998</td>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Media traversal services-private</td>
<td>Edge or Combo</td>
<td>Media traversal (private)</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Media traversal services public interface IP</td>
<td>23002 – 33998</td>
<td>TCP/UDP</td>
<td>Inbound</td>
<td>Media traversal services-public</td>
<td>Edge or Combo</td>
<td>Media traversal (public)</td>
</tr>
<tr>
<td>Media traversal services public interface IP</td>
<td>23002 – 33998</td>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Media traversal services-public</td>
<td>Edge or Combo</td>
<td>Media traversal (public)</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>TURN services public interface IP</td>
<td>60002 – 65535</td>
<td>UDP</td>
<td>Inbound</td>
<td>TURN relay</td>
<td>Edge or Combo</td>
<td>TURN relay</td>
</tr>
<tr>
<td>TURN services public interface IP</td>
<td>60002 – 65535</td>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>Outbound</td>
<td>TURN relay</td>
<td>Edge or Combo</td>
<td>TURN relay</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>TURN services private interface IP</td>
<td>60002 – 65535</td>
<td>UDP</td>
<td>Inbound</td>
<td>TURN relay</td>
<td>Edge or Combo</td>
<td>TURN relay</td>
</tr>
<tr>
<td>TURN services private interface IP</td>
<td>60002 – 65535</td>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>Outbound</td>
<td>TURN relay</td>
<td>Edge or Combo</td>
<td>TURN relay</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>TURN services public interface IP</td>
<td>3478</td>
<td>UDP</td>
<td>Inbound</td>
<td>TURN</td>
<td>Edge or Combo</td>
<td>TURN</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>TURN services private interface IP</td>
<td>3478</td>
<td>UDP</td>
<td>Inbound</td>
<td>TURN</td>
<td>Edge or Combo</td>
<td>TURN</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Signaling services public interface IP</td>
<td>1719</td>
<td>UDP</td>
<td>Inbound</td>
<td>Signaling services-public</td>
<td>Edge or Combo</td>
<td>H.323 RAS</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>1719</td>
<td>UDP</td>
<td>Inbound</td>
<td>Signaling services-private</td>
<td>Edge, Core, or Combo</td>
<td>H.323 RAS</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination IP</td>
<td>Destination Port</td>
<td>Protocol</td>
<td>Direction</td>
<td>RealPresence DMA Configuration</td>
<td>Interface</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Signaling services public interface IP</td>
<td>1719, 52000 – 60000</td>
<td>Any Public IP</td>
<td>1719</td>
<td>UDP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>H.323 RAS</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>1719, 52000 – 60000</td>
<td>Any Private IP</td>
<td>1719</td>
<td>UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>H.323 RAS</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>Any</td>
<td>Signaling services public interface IP</td>
<td>1718</td>
<td>UDP</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>Optional H.323 RAS; gatekeeper discovery (multi- and unicast)</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Signaling services public interface IP</td>
<td>1718</td>
<td>UDP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>Optional H.323 RAS; gatekeeper discovery (multi- and unicast)</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Signaling services public interface IP</td>
<td>1720</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>H.323, H.225</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>1720</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>H.323, H.225</td>
</tr>
<tr>
<td>Signaling services public interface IP</td>
<td>52000 – 60000</td>
<td>Any Public IP</td>
<td>1720</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>H.323, H.225</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>52000 – 60000</td>
<td>Any Private IP</td>
<td>1720</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>H.323, H.225</td>
</tr>
<tr>
<td>Signaling services public interface IP</td>
<td>35001 – 40000</td>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>H.323 dynamic ports (H.245)</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>35001 – 40000</td>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>H.323 dynamic ports (H.245)</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Signaling services public interface IP</td>
<td>35001 – 40000</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Edge or Combo</td>
<td>H.323 dynamic ports (H.245)</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>35001 – 40000</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Edge, Core, or Combo</td>
<td>H.323 dynamic ports (H.245)</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination IP</td>
<td>Destination Port</td>
<td>Protocol</td>
<td>Direction</td>
<td>RealPresence DMA Configuration</td>
<td>Interface</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------</td>
<td>----------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>5060, 5061, 13001 – 23000</td>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Signaling services-private</td>
<td>SIP outbound ports (private)</td>
</tr>
<tr>
<td>Signaling services public interface IP</td>
<td>5060, 5061, 13001 – 23000</td>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Edge or Combo</td>
<td>Signaling services-public</td>
<td>SIP outbound ports (public)</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Signaling services public interface IP</td>
<td>5060</td>
<td>TCP/UDP</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Signaling services-public</td>
<td>SIP signaling (default); other ports can be configured in SIP Settings</td>
</tr>
<tr>
<td>Any Public IP</td>
<td>&gt;1023</td>
<td>Signaling services public interface IP</td>
<td>5061</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge or Combo</td>
<td>Signaling services-public</td>
<td>SIP signaling TLS (default); other ports can be configured in SIP Settings</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>5060</td>
<td>TCP/UDP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Signaling services-private</td>
<td>SIP signaling (default); other ports can be configured in SIP Settings</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>5061</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Signaling services-private</td>
<td>SIP signaling TLS (default); other ports can be configured in SIP Settings</td>
</tr>
<tr>
<td>Signaling services public interface IP</td>
<td>&gt;1023</td>
<td>customerusagedata.tacollection.polycom.com</td>
<td>8443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Signaling services-public</td>
<td>Signaling services (public) communication with Poly Analytics Service</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>&gt;1023</td>
<td>RealPresence ContentConnect</td>
<td>8443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Signaling services-private</td>
<td>Signaling services (private) communication with RealPresence ContentConnect</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>&gt;1023</td>
<td>RealPresence ContentConnect</td>
<td>5060, 5061</td>
<td>TCP</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Signaling services-private</td>
<td>Signaling services (private) communication with RealPresence ContentConnect</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination IP</td>
<td>Destination Port</td>
<td>Protocol</td>
<td>Direction</td>
<td>RealPresence DMA Configuration</td>
<td>Interface</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>RealPresence ContentConnect</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>5060, 5061</td>
<td>TCP</td>
<td>Inbound</td>
<td>Core or Combo</td>
<td>Signaling services private</td>
<td>Signaling services (private) communication with RealPresence ContentConnect</td>
</tr>
<tr>
<td>Other RealPresence DMA nodes Management services IPs</td>
<td>8989</td>
<td>Management services interface IP</td>
<td>8989</td>
<td>UDP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Supercluster communication (core) HA communication (edge, core, or combo)</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>8989</td>
<td>Other RealPresence DMA nodes Management services IPs</td>
<td>8989</td>
<td>UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Supercluster communication (core) HA communication (edge, core, or combo)</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>DNS Servers</td>
<td>53</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>DNS queries.</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>80</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>HTTP: Redirects to 8443 (HTTP access is not allowed)</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>8080</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>HTTP: Redirects to 8443 (HTTP access is not allowed) Used for uploading upgrade packages and backups; during upgrades, the progress page is served from this port</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>443</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>HTTPS; redirects to 8443 Management interface access</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>8443</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Management/API</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>Any Private IP</td>
<td>8443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Management/API</td>
</tr>
<tr>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination IP</td>
<td>Destination Port</td>
<td>Protocol</td>
<td>Direction</td>
<td>RealPresence DMA Configuration</td>
<td>Interface</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------</td>
<td>------------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------------------------</td>
<td>-------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>Active Directory Server</td>
<td>3268, 3269</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Active Directory integration Global Catalog</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>Active Directory server IP</td>
<td>389</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>LDAP Active Directory Integration</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>Microsoft Active Directory Server IP</td>
<td>636</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Microsoft Active Directory integration</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>514, 52000 – 60000</td>
<td>Syslog server IP</td>
<td>514</td>
<td>UDP/TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>Log forwarding</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>123, 52000 – 60000</td>
<td>NTP Server IP</td>
<td>123</td>
<td>UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>NTP (private only); available only if an NTP server is specified in Time Settings</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>52000 – 60000</td>
<td>RealPresence Resource Manager IP</td>
<td>3333, 9333</td>
<td>TCP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>RealPresence Resource Manager licensing; licensing on Edge is optional</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>161</td>
<td>UDP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>SNMP (private only); default port; can be changed or disabled</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>162, 52000 – 60000</td>
<td>SNMP Trap Receiver IP</td>
<td>162</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>SNMP notifications (Traps or Informs) Used if SNMP is enabled and configured to send notifications, or if system is monitored with a RealPresence Resource Manager system</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>&gt;1023</td>
<td>Management services interface IP</td>
<td>22</td>
<td>TCP</td>
<td>Inbound</td>
<td>Edge, Core, or Combo</td>
<td>Management services</td>
<td>SSH (private only); only available if Linux console access is enabled</td>
</tr>
</tbody>
</table>
You can configure a RealPresence DMA system in different ways with a variety of services enabled or disabled. Due to the configurable nature of the RealPresence DMA system, required ports may vary. The RealPresence DMA system web interface provides a list of all configured ports (Service Config > System Port Ranges). From the System Port Ranges page, a firewall administrator can determine which ports a RealPresence DMA system uses for its particular configuration and for which services.

Even though a RealPresence DMA system may have ports open to enable some services or features, internal security measures are often employed to validate the traffic on those ports to secure them wherever possible. Note that a greater number of simultaneous calls requires more ports to be open, so decreasing the number of open ports may reduce the number of calls that can take place.

The following table provides further details about how to calculate required ports:

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Direction</th>
<th>RealPresence DMA Configuration</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management services interface IP</td>
<td>&gt;1023</td>
<td>RealPresence Collaboration Server management IP</td>
<td>80, 8080, 443</td>
<td>TCP</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Management services</td>
<td>Management services communication with RealPresence Collaboration Server</td>
</tr>
<tr>
<td>RealPresence Web Suite IP</td>
<td>&gt;1023</td>
<td>Signaling services private interface IP</td>
<td>8843</td>
<td>TCP</td>
<td>Inbound</td>
<td>Core or Combo</td>
<td>Signaling services private</td>
<td>WebRTC</td>
</tr>
<tr>
<td>Signaling services private interface IP</td>
<td>8843, 52000 – 60000</td>
<td>RealPresence Web Suite IP</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Signaling services private</td>
<td>WebRTC</td>
</tr>
<tr>
<td>Poly ContentConnect IP</td>
<td>443</td>
<td>Management services interface IP</td>
<td>8443 TCP (TLS)</td>
<td>Inbound</td>
<td>Core or Combo</td>
<td>Management services</td>
<td>Poly ContentConnect communication</td>
<td></td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>8443</td>
<td>Poly ContentConnect IP</td>
<td>443</td>
<td>TCP (TLS)</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Management services</td>
<td>Poly ContentConnect communication</td>
</tr>
<tr>
<td>RealPresence Resource Manager IP</td>
<td>&gt;1023</td>
<td>Management services interface IP</td>
<td>4449</td>
<td>TCP</td>
<td>Inbound</td>
<td>Core or Combo</td>
<td>Management services</td>
<td>Legacy LDAP port for Poly CMA and RealPresence Resource Manager integration</td>
</tr>
<tr>
<td>Management services interface IP</td>
<td>5986, 52000 – 60000</td>
<td>Windows Active Directory server IP</td>
<td>5986</td>
<td>TCP (TLS)</td>
<td>Outbound</td>
<td>Core or Combo</td>
<td>Management services</td>
<td>WinRM 2.0 communication during Poly contact creation in Active Directory</td>
</tr>
<tr>
<td>Any Private IP</td>
<td>Any</td>
<td>Management services interface IP</td>
<td>53</td>
<td>TCP/UDP</td>
<td>Inbound</td>
<td>Core</td>
<td>Management services</td>
<td>DNS; only available if the embedded DNS server is enabled</td>
</tr>
</tbody>
</table>
Calculations for Number of Required Ports

<table>
<thead>
<tr>
<th>Information Type</th>
<th>H.323 Dynamic Ports</th>
<th>SIP Dynamic Ports (public)</th>
<th>SIP Dynamic Ports (private)</th>
<th>Media Traversal Dynamic Ports (public) (edge or combo config)</th>
<th>Media Traversal Dynamic Ports (private) (edge or combo config)</th>
<th>Access Proxy (edge or combo config)</th>
<th>System Ephemeral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports used per call</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>10</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of calls</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Total ports required</td>
<td>3x</td>
<td>3x</td>
<td>3x</td>
<td>10x</td>
<td>10x</td>
<td>3000</td>
<td>3000</td>
</tr>
</tbody>
</table>

View System Port Ranges

You can view all current port assignments for a RealPresence DMA system from the management user interface.

Port assignments must be configured on the individual settings page for each service (for example, Access Proxy Settings).

Procedure

» Go to Service Config > System Port Ranges.

The following port information displays:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The service (function) that uses the port or port range.</td>
</tr>
<tr>
<td>First Port</td>
<td>For a port range, the beginning port in the range.</td>
</tr>
<tr>
<td>Last Port</td>
<td>For a port range, the ending port in the range.</td>
</tr>
<tr>
<td>&lt;Network Interface&gt;</td>
<td>The network interface(s) to which the listed service is assigned.</td>
</tr>
</tbody>
</table>
DNS Records for the RealPresence DMA System

Topics:

- Required DNS Records
- Optional DNS Records
- Verify that DNS Works for All Addresses

The RealPresence DMA system uses DNS resource records configured on your DNS server(s). Some of the DNS records are required, while others may be optional.

Note: If you are not familiar with DNS administration, the creation of various kinds of DNS resource records (A/AAAA, NAPTR, NS, and SRV), your enterprise's DNS implementation, and tuning for load balancing (if needed), consult with the DNS system administrator.

The RealPresence DMA system requires the following records on your DNS server(s):

- A and/or AAAA records for IPv4 and IPv6
- Corresponding PTR records for the A and/or AAAA records

You may also need to create additional DNS records for your Microsoft Active Directory server (if different from the DNS server), SIP proxy, H.323 gatekeeper, and embedded DNS servers if you use these services.

Related Links
View the Site Information on page 421

Required DNS Records

Your RealPresence DMA system must be accessible by its host name(s), not just its IP address(es), so you must create A and/or AAAA records for IPv4 and IPv6, respectively, as well as the corresponding PTR records, on your DNS server(s).

A and/or AAAA records map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address. The corresponding PTR records allow reverse DNS resolution of the system's physical or virtual host name(s).

DNS allows you to associate multiple DNS names with a single IP address by creating multiple A records or AAAA records that resolve to the same IP address. However, on the authoritative DNS servers for all RealPresence DMA clusters, you need to define one-to-one relationships between each cluster's FQDN and its management IP address. Additionally, each cluster's host name must match the first node of the FQDN associated with its management IP address.

Note: Depending on local DNS configuration, a host name could be the RealPresence DMA system's FQDN or a shorter name that DNS can resolve.
DNS allows you to associate multiple aliases with a given name (which would be associated with one or more IP addresses). DNS also allows you to associate multiple IP addresses with a single DNS name by creating multiple PTR records that resolve to the same DNS name.

Optional DNS Records

In addition to the required DNS records for the RealPresence DMA system, you need to create DNS records for SIP proxy, H.323 gatekeeper, and embedded DNS servers if you use these services.

Add DNS Records for SIP Proxy

To use your RealPresence DMA system as a SIP proxy server, create the following DNS records (for each cluster in a supercluster, if applicable):

- SRV records for each transport protocol that identify the host names of the SIP proxies that service a particular domain. Configure these statically to point to the host names of the call servers in the domain. Here are example records for two clusters:

  _sips._tcp.example.com. 86400 IN SRV 10 1001 5061 dma-asia.example.com.
  _sips._tcp.example.com. 86400 IN SRV 10 1002 5061 dma-europe.example.com.
  _sip._tcp.example.com. 86400 IN SRV 20 1002 5060 dma-europe.example.com.
  _sip._udp.example.com. 86400 IN SRV 30 1001 5060 dma-asia.example.com.
  _sip._udp.example.com. 86400 IN SRV 30 1002 5060 dma-europe.example.com.

- Optionally, NAPTR records that describe the transport protocols supported by the SIP proxies at a domain and identify the preferred protocol. Configure these statically to match the system's SIP transport protocol configuration.

- To enable access from the public Internet, create corresponding SRV records, visible from outside the firewall, for the public address of each SIP session border controller (SBC).

For more information about the use of DNS in SIP, refer to RFCs 3263 and 2782.

Add DNS Records for the H.323 Gatekeeper

To use your RealPresence DMA system as an H.323 gatekeeper, create the following DNS records (for each cluster in a supercluster, if applicable):

- SRV records that identify the host names of the gatekeepers that service a particular domain. These records are necessary to enable the optional inbound URL dialing feature. Configure them statically to point to the host names of the call servers in the domain. Here are example records for two clusters:

  _h323ls._udp.example.com. 86400 IN SRV 0 1 1719 dma-asia.example.com.
  _h323ls._udp.example.com. 86400 IN SRV 0 1 1719 dma-europe.example.com.
  _h323cs._tcp.example.com. 86400 IN SRV 0 1 1720 dma-asia.example.com.
  _h323cs._tcp.example.com. 86400 IN SRV 0 1 1720 dma-europe.example.com.
To enable access from the public Internet, create corresponding SRV records, visible from outside the firewall, for the public address of each H.323 session border controller (SBC).

For more information about the use of DNS in H.323, refer to the H.323 specification, Annex O, and the H.225.0 specification, Appendix IV.

Add DNS Records for the Optional Embedded DNS Server

To support DNS publishing by your RealPresence DMA system's embedded DNS servers, a DNS NS record is needed for the physical host name of each server in each cluster in the supercluster.

These records identify the RealPresence DMA system's embedded DNS servers as authoritative for the specified logical host name. The logical host name you specify is the one in the Call server sub-domain controlled by RealPresence DMA field on the Embedded DNS page. The following example records are for two dual-server clusters:

```
callservers.example.com. 86400 IN NS dma-asia-server1.example.com.
callservers.example.com. 86400 IN NS dma-asia-server2.example.com.
callservers.example.com. 86400 IN NS dma-europe-server1.example.com.
callservers.example.com. 86400 IN NS dma-europe-server2.example.com.
```

**Note:** Do not create NS records for virtual host names.

Your enterprise DNS must also have the zone `callservers.example.com` defined and be configured to forward requests for names in that zone to any of the clusters in the supercluster. The way you do this depends on the DNS server software being used.

Queries to the enterprise DNS for `callservers.example.com` are referred to the specified RealPresence DMA clusters. Their embedded DNS servers create and manage A records for each site in the site topology. When responsibility for a site moves from one cluster to another, the A records are updated so that the site's domain name is mapped to the new cluster.

Verify that DNS Works for All Addresses

To confirm that DNS can resolve all the host names or FQDNs, you must ping each of them from the management interface, or from a command prompt on the PC you’re using to access the system or from one of the clusters you’re setting up.

**Note:** If you have access to a Linux PC and are familiar with the `dig` command, you can use it to query the enterprise DNS server to verify that all of the records (A/AAAA, NS, and SRV) are present and accurate.

**Procedure**

1. Go to Admin > Troubleshooting Utilities > Ping.
2. Enter an IP address or host name.
   You can also enter an FQDN.
3. Select the Ping type the system will perform (ping or arping).
4. Optionally, select Use specified network interface and select a network interface from the drop-down list.
   The ping or ARP request will originate from the IP address of the network interface you select.
5. Click **Ping** to confirm that DNS can resolve the host name or FQDN that you entered.
Server Configuration

Topics:

- Server Settings
- Signaling Settings
- High Availability Settings
- Security Settings
- Security Certificates
- History Retention Settings
- Superclustering

This section provides an introduction to the RealPresence DMA system configuration.
Server Settings

Topics:

- Network Settings
- Run the Network Configuration Utility
- Configure Time Settings
- Configure Logging Settings
- Configure Alert Settings
- Changing the Linux Root Password
- Changing the Linux Remote Password
- Usage Data

Some of the following RealPresence DMA system settings can be configured during the system installation.

The administrator can revise the server settings as needed.

Network Settings

Some network settings are configured during system installation and rarely need to be changed.

Revising some network settings (host names, IP addresses, or domains) requires a system restart and terminates all active conferences.

The RealPresence DMA system needs to be accessible by its host name(s), not just its IP address(es), so you must create A and/or AAAA records for IPv4 and IPv6, respectively, as well as the corresponding PTR records, on your DNS server(s). A/AAAA records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory, as are the corresponding PTR records that allow reverse DNS resolution of the system's physical or virtual host name(s).

If the RealPresence DMA system uses a CA-provided identity certificate, changing host names or IP addresses also requires that you update the certificate. If the revised settings require a new certificate, the system will automatically generate a new self-signed certificate.

You can't configure or revise network settings under the following circumstances:

- While the system is part of a supercluster - you must first leave the supercluster and, if the cluster is responsible for any territories (as primary or backup), reassign those territories. After the making the network changes, the system can rejoin the supercluster.
- When the system is integrated with a RealPresence Resource Manager system - you must first terminate the integration. After the making the network changes, the system can reintegrate with the RealPresence Resource Manager system.
- When the system is configured for high availability (HA) - you must disable HA before you revise any network settings. After the making the network changes, HA can be re-enabled.
Configure General System Network Settings

Some of the General System Network Settings are configured during system installation but can be changed when necessary.

The General System Network Settings apply to the entire RealPresence DMA system and aren't specific to management or signaling interfaces.

**Note:** Changing some network settings (host names, IP addresses, or domains) requires a system restart and terminates all active conferences.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Complete the fields described in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System IP type</td>
<td>Displays which type of addressing is currently enabled (IPv4 and/or IPv6).</td>
</tr>
<tr>
<td>Host name</td>
<td>The host name of the system.</td>
</tr>
<tr>
<td></td>
<td>If a DHCP server assigned the host name during system installation, you</td>
</tr>
<tr>
<td></td>
<td>can select <strong>Override DHCP Settings</strong> and enter a host name that overrides</td>
</tr>
<tr>
<td></td>
<td>the DHCP-assigned host name.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain for the system. This is combined with the host name to form the</td>
</tr>
<tr>
<td></td>
<td>FQDN. For instance:</td>
</tr>
<tr>
<td></td>
<td>Host name: dma1</td>
</tr>
<tr>
<td></td>
<td>Domain: callservers.example.com</td>
</tr>
<tr>
<td></td>
<td>FQDN: dma1.callservers.example.com</td>
</tr>
<tr>
<td></td>
<td>If a DHCP server assigned the domain during system installation, you can</td>
</tr>
<tr>
<td></td>
<td>select <strong>Override DHCP Settings</strong> and enter a domain that overrides the</td>
</tr>
<tr>
<td></td>
<td>DHCP-assigned domain.</td>
</tr>
<tr>
<td>DNS search domains</td>
<td>One or more FQDNs, separated by commas or spaces. The domain you enter for</td>
</tr>
<tr>
<td></td>
<td>the system is added automatically.</td>
</tr>
<tr>
<td></td>
<td>If a DHCP server assigned DNS search domains during system installation,</td>
</tr>
<tr>
<td></td>
<td>you can select <strong>Override DHCP Settings</strong> and enter DNS search domains that</td>
</tr>
<tr>
<td></td>
<td>override the ones assigned by DHCP.</td>
</tr>
<tr>
<td>DNS 1</td>
<td>IP addresses of up to three domain name servers. At least one DNS server</td>
</tr>
<tr>
<td></td>
<td>is required.</td>
</tr>
<tr>
<td>DNS 2</td>
<td>DNS queries on any configured network interface will be sent to the same</td>
</tr>
<tr>
<td>DNS 3</td>
<td>DNS name servers (in order).</td>
</tr>
<tr>
<td></td>
<td>If a DHCP server assigned DNS 1 during system installation, you can select</td>
</tr>
<tr>
<td></td>
<td><strong>Override DHCP Settings</strong> and enter a primary DNS that overrides the</td>
</tr>
<tr>
<td></td>
<td>the one assigned by DHCP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system uses the secondary DNS server only if the primary DNS</td>
</tr>
<tr>
<td></td>
<td>server is unreachable and uses the tertiary DNS server only if the primary</td>
</tr>
<tr>
<td></td>
<td>and secondary servers are unreachable.</td>
</tr>
</tbody>
</table>

**Server Settings**
### Configure Network Interface Settings

You can configure general, IPv4, and IPv6 settings for any network interface.

Note that **Link Settings** and **LAN Security Settings** can be configured only for NIC interfaces.

Changing some network settings (host names, IP addresses, or domains) requires a system restart and terminates all active conferences.

**Note:** If you configure any interface as **STATIC**, you can’t configure any other interface as DHCP. If you configure any interface as **DHCP**, you can’t configure another interface.

#### Procedure

1. Go to **Admin > Server > Network Settings**.
2. In the **Network Interface Settings** section, select an interface to configure and click the **Edit Selected Interface** button.
3. Configure the settings for the network interface as described in the following table:

<table>
<thead>
<tr>
<th>Generic NIC</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable</td>
<td>If an interface has services assigned to it, it cannot be disabled. Services must first be re-assigned to another interface.</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>The name of a NIC network interface isn’t editable. The names of bonded and VLAN interfaces are generated.</td>
</tr>
<tr>
<td></td>
<td>MAC address</td>
<td>The MAC address of the network interface card.</td>
</tr>
</tbody>
</table>
### IPv4 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are <strong>STATIC</strong> or <strong>DHCP</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> If you configure any interface as <strong>STATIC</strong>, you can’t configure any other interface as <strong>DHCP</strong>. If you configure any interface as <strong>DHCP</strong>, you can’t configure another interface.</td>
</tr>
<tr>
<td>IPv4 address/prefix length*</td>
<td>IPv4 address and the CIDR (Classless Inter-Domain Routing) prefix size of the interface.</td>
</tr>
<tr>
<td>IPv4 gateway*</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>MTU size</td>
<td>The Maximum Transmission Unit size for the network interface. The default size set by Linux is 1500. It’s recommended that you leave this field blank to use the system’s default value.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> If you set the MTU size to a value not supported by your network, you may lose access to the RealPresence DMA system web interface. Additionally, all network devices (switches, routers, other RealPresence DMA systems, MCUs, and others) that exchange network packets through the configured interface must have the same MTU size setting. If these other devices are not configured with the same MTU size, the connection to the RealPresence DMA system won’t work.</td>
</tr>
<tr>
<td>NAT address</td>
<td>Specify a NAT address only if services are assigned to the network interface.</td>
</tr>
<tr>
<td></td>
<td>If you deploy the system behind a firewall and your network requires a NAT address for public access, enter the public IP address that’s used to access this interface.</td>
</tr>
<tr>
<td></td>
<td>For High Availability configurations, if you deploy the systems behind a firewall and your network requires a NAT address, map the NAT address to the virtual IP address rather than the physical address for each interface that has assigned public signaling services and public media traversal services.</td>
</tr>
</tbody>
</table>

### IPv6 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are <strong>STATIC</strong>, <strong>SLAAC</strong>, or <strong>DHCP6</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> If you configure any interface as <strong>STATIC</strong>, you can’t configure any other interface as <strong>DHCP6</strong>. If you configure any interface as <strong>DHCP6</strong>, you can’t configure another interface.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bit in the routing prefix mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which isn’t visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the local link.</td>
</tr>
</tbody>
</table>

### Link Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonegotiation</td>
<td>Turn on <strong>Auto-negotiation</strong> or set <strong>Speed</strong> and <strong>Duplex</strong> manually. <strong>Note:</strong> Autonegotiation is required if your network is 1000Base-T. Don't select 10000 unless you’re certain your hardware platform supports it.</td>
</tr>
<tr>
<td>Speed</td>
<td></td>
</tr>
<tr>
<td>Duplex</td>
<td></td>
</tr>
</tbody>
</table>

### LAN Security Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable 802.1x</td>
<td>Enables the system to authenticate this network interface to the LAN. Depending on the authentication method, the access credentials required may be either a user name and password or a security certificate. <strong>Caution:</strong> In a network that requires 802.1x authentication for servers (this is rarely the case), incorrect settings in this section and, if applicable, lack of the proper certificate(s) can make the system unreachable. Recovering from this situation requires connecting a laptop to the system using a crossover cable in order to access it.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name with which the system may authenticate this interface.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user name entered above.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>EAP Method</td>
<td>The Extensible Authentication Protocol method used to establish trust with the authentication server (also known as the outer authentication protocol).</td>
</tr>
<tr>
<td>Protocol</td>
<td>When a TLS tunnel is established with the authentication server, the protocol used within the tunnel (this is also known as the inner authentication protocol).</td>
</tr>
</tbody>
</table>

4. **Click OK** to save the settings.
Configure Service Settings

If your RealPresence DMA system has a core configuration, you can assign management and signaling services to any interface that is enabled and configured with either a static or dynamic IP address.

The services can be assigned to the same or different interfaces.

If your RealPresence DMA system has an edge configuration, in addition to assigning management services to an interface, you can also assign the following edge-related services to network interfaces and specify a private and public IP address for each interface.

- Signaling
- Media Traversal
- Access Proxy
- TURN

Interfaces without services assigned may still be used in high availability (HA) configurations for HA communication between systems.

Procedure

1. Go to Admin > Server > Network Settings.
2. Click Services.
3. Configure the management and signaling settings as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Services</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>The interface the RealPresence DMA system uses for management traffic.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets associated with management traffic (including communications to other RealPresence DMA systems). The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
<tr>
<td>Allow edge services</td>
<td>When selected, this option enables edge-related services to be configured on network interfaces.</td>
</tr>
<tr>
<td><strong>Signaling Services</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>The private interface the RealPresence DMA system uses for signaling traffic to internal network endpoints or other devices. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
<tr>
<td>Public</td>
<td>The public interface the RealPresence DMA system uses for signaling traffic. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
<tr>
<td>Field</td>
<td>Descriptions</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>DSCP</strong></td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets for signaling traffic. The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
<tr>
<td><strong>Media Traversal Services</strong> (available only on edge-configured systems)</td>
<td><strong>Private</strong></td>
</tr>
<tr>
<td>Interface</td>
<td>The private interface the RealPresence DMA system uses for media traffic to internal network endpoints or other devices. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets for media traffic. The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
<tr>
<td><strong>Access Proxy Services</strong> (available only on edge-configured systems)</td>
<td><strong>Private</strong></td>
</tr>
<tr>
<td>Interface</td>
<td>The private interface the RealPresence DMA system uses for access proxy traffic to internal network endpoints or other devices. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets for media traffic. The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets for access proxy traffic. The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0.</td>
</tr>
</tbody>
</table>

### TURN Services

<table>
<thead>
<tr>
<th>Interface</th>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The private interface the RealPresence DMA system uses for TURN traffic to internal network WebRTC endpoints. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
<td>The public interface the RealPresence DMA system uses for TURN traffic. This may be a network interface card, a VLAN interface, or a bonded interface.</td>
</tr>
</tbody>
</table>

| DSCP | The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers on outbound packets for TURN traffic. The DSCP value is used to classify packets for Quality of Service (QoS) purposes. If you are not sure what value to use, leave the default of 0. | |

4. Click OK to save the settings and restart the system.

### Routing Configuration

If your network configuration requires specific routing for some subnet(s), you can use static routes to handle the requirements.

#### Add a Static Route

You can configure static route settings only if they’re valid for the current network settings.

If you need to change both the network settings and routing configuration, change the network settings first to prevent system errors.

**Procedure**

1. Go to Admin > Server > Network Settings.
2. Click Routing Configuration.
3. Select the Default gateway device.
   - The **Default gateway device** is the network interface designated as the default route when no other routing rules match the destination network address.
4. Click Add Route.
5. Complete the fields in the following table as required:


### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the interface for this route.</td>
</tr>
<tr>
<td>Subnet</td>
<td>The target address prefix for the route. It should consist of a network specification, for example, 192.168.9.0 or 192.168.0.0.</td>
</tr>
<tr>
<td>Prefix length</td>
<td>The Classless Inter-Domain Routing (CIDR) prefix size value (the number of leading 1 bit in the routing prefix mask). This value, together with the Subnet address, define the destination network for this route.</td>
</tr>
<tr>
<td>Via</td>
<td>IP address of the next hop or gateway for this route.</td>
</tr>
</tbody>
</table>

6. Click OK.

   The static route displays in the **Static Routes** table.

7. Repeat the preceding steps to add more routes.

8. When you have added all necessary routes, click **OK** to save the routes and restart the system.

### Delete a Static Route

You can delete static routes as needed.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Click **Routing Configuration**.
3. Select a static route from the list and click **Delete Selected Route** to delete it.
4. Click **OK**.

### Bonded and VLAN Interfaces

The RealPresence DMA system supports the use of logical interfaces in addition to physical network interfaces.

You can add bonded and VLAN interfaces that can provide increased bandwidth and redundancy capabilities for your network interfaces.

A bonded interface can be configured to combine two or more physical NICs into a single logical network interface. This is also known as Link Aggregation. When bonded, the NICs appear to be the same physical device. Bonding requires a switch that supports and is configured for link aggregation control protocol (LACP), as described in IEEE 802.3ad.

VLAN interfaces can be created by splitting a single NIC link into multiple logical links. The physical NIC defines the VLAN interfaces (for example, `eth1.1`, `eth1.2`, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

You can assign RealPresence DMA system services such as management and signaling to both physical and logical interfaces. Both types of interfaces can be used for communication between two RealPresence DMA systems configured for High Availability.

Note that the NICs associated with a logical interface shouldn’t be:

- Assigned IP addresses
- Used in firewall rules
- Used in network packet captures
- Used in traceroute
- Used in ping

**Add a Bonded Interface**

A bonded interface can increase available bandwidth and provide NIC failover protection.

You can add a bonded interface to combine two or more NICs into a single logical network connection. The logical network interface is typically represented by `bond0`, `bond1`...`bondn`. The NICs (`eth1`, `eth2`, etc.) are considered slaves of the bonded interface.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Under **ACTIONS**, click **Add Bonded Interface**.
3. Configure the settings for the bonded interface as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system generates the name of the interface based on the number of bonded interfaces already configured, starting with <code>bond0</code> and incrementing by 1, for example, <code>bond1</code>, <code>bond2</code>, etc.</td>
</tr>
<tr>
<td>Enable</td>
<td>Select the check box if the bonded interface will be assigned IP addresses. If the bonded interface is configured at the switch to deliver a VLAN trunk, complete the necessary configuration and then uncheck the <strong>Enable</strong> check box before clicking <strong>OK</strong> to save the interface. You’ll add one or more VLAN interfaces later, which will automatically enable the bonded interface.</td>
</tr>
<tr>
<td>Available NICs</td>
<td>The interfaces available for aggregation.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bonding policy</td>
<td>This policy is applied to the bonded interface but the switch must be configured to support the policy you select. The following bonding policy values are available: <strong>balance-rr</strong> - Sets a round-robin policy for fault tolerance and load balancing. Transmissions are received and sent out sequentially on each bonded slave interface beginning with the first one available.  <strong>active-backup</strong> - Sets an active-backup policy for fault tolerance. Transmissions are received and sent out via the first available bonded slave interface. Another bonded slave interface is only used if the active bonded slave interface fails.  <strong>balance-xor</strong> - Sets an XOR (exclusive-or) policy for fault tolerance and load balancing. Using this method, the interface matches the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface.  <strong>broadcast</strong> - Sets a broadcast policy for fault tolerance. All transmissions are sent on all slave interfaces.  <strong>802.3ad</strong> - Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator. Requires a switch that is 802.3ad compliant.  <strong>balance-tlb</strong> - Sets a Transmit Load Balancing (TLB) policy for fault tolerance and load balancing. The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.  <strong>balance-alb</strong> - Sets an Adaptive Load Balancing (ALB) policy for fault tolerance and load balancing. Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through ARP negotiation. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.</td>
</tr>
<tr>
<td>Link monitoring</td>
<td><strong>balance-tlb</strong> - Sets a TLB policy for fault tolerance and load balancing. The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.  <strong>balance-alb</strong> - Sets an ALB policy for fault tolerance and load balancing. Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through ARP negotiation. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring frequency</td>
<td>When selected, enables the RealPresence DMA system to monitor the physical NICs to ensure they’re working. Primarily used for bonding policies that provide redundancy.</td>
</tr>
<tr>
<td>Link up delay (ms)</td>
<td>If Link monitoring is selected, specify how often the system checks the physical NICs. A recommended starting point is 100 ms.</td>
</tr>
<tr>
<td>Link down delay (ms)</td>
<td>The length of time the system waits before enabling a link connection after a restart; must be a multiple of the Monitoring frequency value. Entering zero disables the link up delay.</td>
</tr>
</tbody>
</table>

### IPv4 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are STATIC or DHCP.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

### IPv6 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are STATIC, SLAAC, or DHCP.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR prefix size value (the number of leading 1 bit in the routing prefix mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

### Edit a Bonded Interface

You can edit the network interface settings for a bonded interface when necessary.

A bonded interface can increase available bandwidth and provide NIC failover protection. You can add a bonded interface to combine two or more NICs into a single logical network connection. The logical network interface is typically represented by `bond0, bond1...bondn`. The NICs (eth1, eth2, etc.) are considered slaves of the bonded interface.
Procedure

1. Go to Admin > Server > Network Settings.
2. Under Network Interface Settings, select the bonded interface to edit.
3. Click the Edit button at the top of the table.
4. Configure the settings for the bonded interface as described in the following table:

### General Bonded

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system generates the name of the interface based on the number of bonded interfaces already configured, starting with bond0 and incrementing by 1, for example, bond1, bond2, etc.</td>
</tr>
<tr>
<td>Enable</td>
<td>Select the check box if the bonded interface will be assigned IP addresses. If the bonded interface is configured at the switch to deliver a VLAN trunk, complete the necessary configuration and then uncheck the <strong>Enable</strong> check box before clicking <strong>OK</strong> to save the interface. You’ll add one or more VLAN interfaces later, which will automatically enable the bonded interface.</td>
</tr>
<tr>
<td>Available NICs</td>
<td>The interfaces available for aggregation.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bonding policy</td>
<td>This policy is applied to the bonded interface but the switch must be configured to support the policy you select.</td>
</tr>
<tr>
<td></td>
<td>The following bonding policy values are available:</td>
</tr>
<tr>
<td></td>
<td><strong>balance-rr</strong> - Sets a round-robin policy for fault tolerance and load balancing. Transmissions are received and sent out sequentially on each bonded slave interface beginning with the first one available.</td>
</tr>
<tr>
<td></td>
<td><strong>active-backup</strong> - Sets an active-backup policy for fault tolerance. Transmissions are received and sent out via the first available bonded slave interface. Another bonded slave interface is only used if the active bonded slave interface fails.</td>
</tr>
<tr>
<td></td>
<td><strong>balance-xor</strong> - Sets an XOR (exclusive-or) policy for fault tolerance and load balancing. Using this method, the interface matches the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface.</td>
</tr>
<tr>
<td></td>
<td><strong>broadcast</strong> - Sets a broadcast policy for fault tolerance. All transmissions are sent on all slave interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>802.3ad</strong> - Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator. Requires a switch that is 802.3ad compliant.</td>
</tr>
<tr>
<td></td>
<td><strong>balance-tlb</strong> - Sets a Transmit Load Balancing (TLB) policy for fault tolerance and load balancing. The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.</td>
</tr>
<tr>
<td></td>
<td><strong>balance-alb</strong> - Sets an Adaptive Load Balancing (ALB) policy for fault tolerance and load balancing. Includes transmit and receive load balancing for IPv4 traffic. Receive load balancing is achieved through ARP negotiation. This mode is only suitable for local addresses known to the kernel bonding module and therefore cannot be used behind a bridge with virtual machines.</td>
</tr>
<tr>
<td>Link monitoring</td>
<td>When selected, enables the RealPresence DMA system to monitor the physical NICs to ensure they’re working. Primarily used for bonding policies that provide redundancy.</td>
</tr>
<tr>
<td>Monitoring frequency (ms)</td>
<td>If <strong>Link monitoring</strong> is selected, specify how often the system checks the physical NICs. A recommended starting point is 100 ms.</td>
</tr>
<tr>
<td>Link up delay (ms)</td>
<td>The length of time the system waits before enabling a link connection after a restart; must be a multiple of the <strong>Monitoring frequency</strong> value. Entering zero disables the link up delay.</td>
</tr>
<tr>
<td>Link down delay (ms)</td>
<td>The length of time the system waits after a link fails before disabling the connection; must be a multiple of the <strong>Monitoring frequency</strong> value. Entering zero disables the link down delay.</td>
</tr>
</tbody>
</table>
## IPv4 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are <strong>STATIC</strong> or <strong>DHCP</strong>.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

## IPv6 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are <strong>STATIC</strong>, <strong>SLAAC</strong>, or <strong>DHCP</strong>.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR (Classless Inter-Domain Routing) prefix size value (the number of leading 1 bit in the routing prefix mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

### Add a VLAN Interface

VLAN interfaces can be created by splitting a single NIC link into multiple logical links.

The physical NIC defines the VLAN interfaces (for example, **eth1.1**, **eth1.2**, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Under **ACTIONS**, click **Add VLAN Interface**.
3. Configure the settings for the VLAN interface as described in the following table:

### General VLAN Interface

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system assigns the name of the VLAN interface when you save the VLAN Interface Settings. The name is a combination of the interface (NIC or bond) on which you create the VLAN interface and the VLAN ID, for example, eth2.1, where eth2 is the parent interface and 1 is the VLAN ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The numeric ID of the VLAN interface. The ID specifies the individual network within the VLAN trunk that the interface will be connected to.</td>
</tr>
<tr>
<td>Interface</td>
<td>The available interfaces (NIC or bond) on which you can create a VLAN interface.</td>
</tr>
</tbody>
</table>

**IP Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are <strong>STATIC</strong> or <strong>DHCP</strong>.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are <strong>STATIC</strong>, <strong>SLAAC</strong>, or <strong>DHCP</strong>.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR prefix size value (the number of leading 1 bit in the routing prefix mask) that define the subnetwork of the system's management or combined interface. Routable anywhere/scoped globally.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Edit a VLAN Interface**

VLAN interfaces can be created by splitting a single NIC link into multiple logical links.

The physical NIC defines the VLAN interfaces (for example, **eth1.1, eth1.2**, etc.), each of which is a logical network interface configured with an IP address. Each VLAN interface is associated with a subnet on a VLAN trunk supplied by a switch that carries VLAN traffic, as described in IEEE 802.1Q. An aggregated link (bonded interface) can also be configured to deliver a VLAN trunk.

**Procedure**

1. Go to **Admin > Server > Network Settings.**
2. Under **Network Interface Settings**, select the VLAN interface to edit.
3. Click the **Edit** button at the top of the table.
4. Configure the settings for the VLAN interface as described in the following table:
General Network Interface

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The RealPresence DMA system assigns the name of the VLAN interface when you save the VLAN Interface Settings. The name is a combination of the interface (NIC or bond) on which you create the VLAN interface and the VLAN ID, for example, eth2.1, where eth2 is the parent interface and 1 is the VLAN ID.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The numeric ID of the VLAN interface. The ID specifies the individual network within the VLAN trunk that the interface will be connected to.</td>
</tr>
<tr>
<td>Interface</td>
<td>The available interfaces (NIC or bond) on which you can create a VLAN interface.</td>
</tr>
</tbody>
</table>

IP Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 boot protocol</td>
<td>The IPv4 boot protocol of the network interface. Options are STATIC or DHCP.</td>
</tr>
<tr>
<td>IPv4 address/prefix length</td>
<td>IPv4 address and CIDR (network mask) that defines the subnetwork of the system's management or combined interface.</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>IPv4 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td>IPv6 boot protocol</td>
<td>The IPv6 boot protocol of the network interface. Options are STATIC, SLAAC, or DHCP.</td>
</tr>
<tr>
<td>IPv6 (global) address/prefix length</td>
<td>IPv6 address and the CIDR prefix size value (the number of leading 1 bits in the routing prefix mask) that define the subnetwork of the system's management or combined interface. Routable anywhere/ scoped globally.</td>
</tr>
<tr>
<td>IPv6 (link-local)</td>
<td>The IPv6 link-local address, which is not visible outside of the link.</td>
</tr>
<tr>
<td>IPv6 gateway</td>
<td>IPv6 address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
</tbody>
</table>

5. Click OK.

Enable IPv6

You can configure your RealPresence DMA network settings to use IPv4 or IPv6 addressing. The system also supports IPv4 and IPv6 addressing simultaneously in a mixed mode environment.

Procedure
1. Go to Admin > Server > Network Settings.
2. Click Enable IPv6.
   A list of all enabled network interfaces displays.
3. For each enabled interface, configure the following settings:
   - **Type**: The system IP address type (STATIC, DHCP6, or SLAAC)
   - IPv6 Address
   - IPv6 Gateway

4. Click OK to enable IPv6 addressing.

### Enable IPv4

You can configure your RealPresence DMA network settings to use IPv4 or IPv6 addressing.

The system also supports IPv4 and IPv6 addressing simultaneously in a mixed mode environment.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Click **Enable IPv4**.
   
A list of all enabled network interfaces displays.
3. For each enabled interface, configure the following settings:
   - **Type**: The system IP address type (STATIC, DHCP)
   - IPv4 Address
   - IPv4 Gateway

4. Click OK to enable IPv4 addressing.

### Edit System Ephemeral Ports

The RealPresence DMA system uses local ephemeral ports to make outbound network connections for transient services and operations not otherwise defined with their own specific port ranges.

For example, when the system contacts another RealPresence DMA system to perform some administrative function (invite the other system into an HA pair, automatically configure VPN tunnel entries, etc.), the first system may use a local ephemeral port to initiate the HTTPS connection to the peer's 8443 port.

The RealPresence DMA default system ephemeral port range is 52000-60000. Changing the default port range is not recommended except when it conflicts with the ports or port ranges of other services (for example, H.323 signaling) after upgrading the RealPresence DMA system software. If a conflict occurs, you can revise the system ephemeral port range to avoid having to change the port ranges of other services that would also require firewall changes.

The system ephemeral port range must be 500 or more ports.

**Procedure**

1. Go to **Admin > Server > Network Settings**.
2. Click **System Ephemeral Ports**.
3. Revise the **First port** and/or the **Last port** as needed.
4. Click OK.
Run the Network Configuration Utility

The Network Configuration Utility (also known as the USB Configuration Utility) is a Java program that you can download and run during initial installation of your RealPresence DMA system or access from the management user interface after initial installation.

The utility enables you to make multiple network configuration changes at one time, then reboot only once. For example, you can add a NIC, change service assignments, and assign an NTP server, then reboot your RealPresence DMA system one time.

During initial installation, you might configure only the management network. After initial installation, you can log into the management user interface and use the Network Configuration Utility to configure the network interface settings for additional NICs.

When you download and run the Network Configuration Utility, it generates a network configuration file and saves it on your local PC or a USB flash drive, depending on where you run the utility. You can upload the file to the RealPresence DMA management user interface and then apply the network configuration settings. If you run the utility from a USB flash drive, you can also apply the network configuration by plugging the USB flash drive into a RealPresence DMA server and rebooting the server. The system will read and apply the network configuration settings from the file.

You can also download a network configuration file that you’ve previously uploaded to the RealPresence DMA management user interface in case you lose the original file.

Procedure

1. Log into the RealPresence DMA management user interface.
2. Go to Admin > Server > Network Configuration Utility.
3. Click Download Network Configuration Utility.
   The RealPresence DMA system downloads a zip folder that includes the utility.
4. Extract the contents of the folder to your local PC or to the root of a USB flash drive.
   If you’ll run the utility from a USB flash drive, you must extract the zip folder to the root of the USB flash drive and not to a folder on the flash drive.
5. Do one of the following to launch the Network Configuration Utility:
   • From a client system running Microsoft Windows, run the dma7000-usb-gui.exe file.
   • From a client system running a Unix-based OS (including Mac), run the runUsbGui.sh file.
6. In the Network Configuration Utility window, click Configure the System Parameters.
7. Click Edit next to the node you want to configure.
8. For first-time setup (FTSU), select Core configuration or Edge configuration.
9. Click Next.
10. Complete the Network, Services, Routing, and NTP settings as needed.
11. Click Done.
   The utility creates a zip file that contains the settings you configured and saves it to the location where you extracted the Network Configuration Utility zip file (folder dma).
12. The Network Configuration Utility window displays and confirms that The USB stick is set to apply system parameters.
   This message applies whether you ran the utility from your local PC or from the root of a USB flash drive.
13. From the Network Configuration Utility window in the management user interface, choose one of the following options:
- **Upload Configuration** - Uploads the network settings zip file that you configured using the utility. You can upload the file from your local Windows client or from a USB flash drive.

- **Download Configuration** - Downloads a network settings file that you previously uploaded to the RealPresence DMA system and save it to a local Windows client or USB flash drive.

- **Apply Configuration** - After uploading a network setting’s zip file, you need to apply the settings to activate them. You can do this when you upload them or at a later time.

- **Delete Configuration** - Deletes a network settings file.

---

### Configure Time Settings

For RealPresence DMA Appliance Edition systems, you can configure time settings with the USB Configuration Utility during first-time setup of your system.

You can change a system’s (or cluster’s) time settings at any time, but note that this requires a system restart and terminates all active conferences.

For RealPresence DMA Virtual Edition systems, time settings are typically inherited from the RealPresence DMA Resource Manager system or manually configured. See the Polycom RealPresence DMA System Getting Started Guide.

**Note:** Polycom recommends specifying at least one but preferably three NTP time servers. You must specify at least one time server before creating or joining a supercluster.

#### Procedure

1. Go to **Admin > Server > Time Settings**.
2. Edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System time zone</td>
<td>Time zone in which the system is located. Polycom recommends selecting the time zone of a specific geographic location (such as America/Denver), not one of the generic GMT offsets (such as GMT+07 POSIX).&lt;br&gt;&lt;br&gt;If you use a generic GMT offset (for instance, to prevent automatic daylight saving time adjustments), note that they use the Linux/Posix convention of specifying how many hours ahead of or behind local time GMT is. Thus, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.</td>
</tr>
<tr>
<td>Use NTP server (recommended)</td>
<td>Specify the <strong>IP Address</strong> or <strong>Host Name</strong> (FQDN) of up to three time servers for maintaining system time&lt;br&gt;&lt;br&gt;Polycor recommends specifying at least one but preferably three NTP time servers.</td>
</tr>
<tr>
<td>Manually set system time</td>
<td>While not recommended, you can manually specify the <strong>System Date</strong> and <strong>System Time</strong>.</td>
</tr>
</tbody>
</table>

3. When finished, click **Update**.
Configure Logging Settings

You can configure the system's logging settings for local and forwarded logs.

Procedure
1. Go to Admin > Server > Logging Settings.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging level</td>
<td>Leave the default, <strong>Debug</strong>, unless advised to change it by Polycom support. <strong>Production</strong> reduces system overhead and log file sizes, but omits information that's useful for troubleshooting. <strong>Verbose debug</strong> is not recommended for production systems.</td>
</tr>
<tr>
<td>Rolling frequency</td>
<td>If rolling the logs daily (the default) produces logs that are too large, shorten the interval.</td>
</tr>
<tr>
<td>Maximum retention time</td>
<td>The number of days to keep log archives.</td>
</tr>
<tr>
<td>Include advanced diagnostics</td>
<td>Select to include advanced diagnostic information in the log archive that allows Polycom to troubleshoot hard-to-reproduce issues. Recommended.</td>
</tr>
</tbody>
</table>
| Local log forwarding   | Select **Enable forwarding** to forward selected log entries to a central log management server. The log management server should be configured to accept log entries via UDP port 514. Specify:  
  - The address of the *Destination server* - It must be running some version of syslog.  
  - The *Syslog facility* - Value used to mark the log messages. The default is *Local0*. If you’re unsure what facility you should use, consult the log management server’s administrator.  
  - The *Logs to forward* - The source log file name is included in each of the forwarded messages. **Note**: The RealPresence DMA system's server.log entries are mapped to syslog-compliant severities (for example, a *warn* message from server.log arrives at the destination server with the syslog-compliant *warn* level, and an *info* message arrives with the *info* level). All other logs being forwarded are assigned the syslog-compliant *notice* severity. Each log message is forwarded with the RealPresence DMA system's timestamp intact. The receiving syslog adds its own timestamp, but preserving the RealPresence DMA - applied timestamp makes it easier to accurately troubleshoot time-sensitive events. |

3. Click **Update**.
4. Click **OK**.
Configure Alert Settings

You can configure thresholds for system alerts, enable or disable certain alerts, and control when they’ll be triggered.

The same threshold settings are used for both system alerts and SNMP alerts.
Certificate-related alert settings cannot be modified.

Procedure

1. Go to Admin > Server > Alert Settings.

The Alert Settings page lists the following alert settings.

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Threshold Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3103</td>
<td>Days until server certificate expires is less than</td>
<td>Alert when there are only this many days until the system's security certificate expires.</td>
</tr>
<tr>
<td>3105</td>
<td>Days until CA certificate expires is less than</td>
<td>Alert when there are only this many days until the server's CA-signed security certificate expires.</td>
</tr>
<tr>
<td>3401</td>
<td>Percentage available disk space is less than</td>
<td>Alert when the percentage of free disk space available on the DMA system falls below this value.</td>
</tr>
<tr>
<td>3404</td>
<td>Percentage log file usage is greater than</td>
<td>Alert when the percentage of the log file storage area used by log data is above this value.</td>
</tr>
<tr>
<td>3405</td>
<td>Percentage CPU utilization is greater than</td>
<td>Alert when system CPU utilization is between this lower limit, and...</td>
</tr>
<tr>
<td></td>
<td>And percentage CPU utilization is less than or equal to</td>
<td>...this upper limit.</td>
</tr>
<tr>
<td>3406</td>
<td>Percentage CPU utilization is greater than</td>
<td>Alert when system CPU utilization is above this value.</td>
</tr>
<tr>
<td>5002</td>
<td>Number of hyperactive, blacklisted endpoints is greater than</td>
<td>Alert when the number of registered endpoints that are blacklisted for sending too much H.323 traffic is above this value.</td>
</tr>
</tbody>
</table>

2. To enable an alert, mark the associated check box.
3. To change the Threshold Value, make sure the associated check box is marked and then use the arrows next to each field or enter a new number to change the default value.
4. Click the Update button to save your changes.
5. To revert your changes, click Restore Defaults.

When you click Restore Defaults, all values return to their factory defaults.
Changing the Linux Root Password

Enterprise and local Administrators can change the Linux OS root password for the RealPresence DMA system without entering a shell interface.

In normal system operations, RealPresence DMA users, including Administrators, don't need to know or use the Linux root password. However, if the root password has been compromised or if corporate security policies require changing all system passwords at certain intervals or after specific events occur, you can change the root password.

Consider the following details before changing the Linux root password:

▪ Only Administrators may change the Linux root password. The menu option doesn't display to Auditors, Provisioners, or users without an assigned role.
▪ You must log in to the physical address of a RealPresence DMA server to change its Linux root password:
  ◦ In a two-server cluster, you must log in to each server to change its root password.
  ◦ Although not required, Polycom recommends that the two servers have the same Linux root password.
▪ Password complexity rules are based on the local password policy settings, with the following exceptions:
  ◦ The Linux root password doesn't expire.
  ◦ Previously used root passwords can be reused.
▪ You can attempt to change the root password only once per minute.
▪ Upgrading the RealPresence DMA system software doesn't change the root password.
▪ If you restore the RealPresence DMA system from a backup file and select the IP network, certificate, security and licensing configuration system backup components, the Linux root password of the restored system will be the same as the root password of the system at the time you created the backup.

Caution: If you change the Linux root password, Polycom Global Services can't access the operating system of your RealPresence DMA system. As a result, support services may be limited.

Related Links
Configure Local Password Settings on page 484

Change the Linux Root Password

You can change the Linux OS root password for the RealPresence DMA system from the management user interface.

Procedure
1. Go to Admin > Server > Change Linux Root Password.
2. Complete the password fields as follows:
   ▪ Old password - If the Linux root password has not been changed since the system was installed, leave this field blank. If the Linux root password has been changed one or more times, enter the current password.
• New password - Enter the new root password.
• Confirm new password - Re-enter the new root password.

3. Click OK.

Changing the Linux Remote Password

If you have enabled Secure Shell (SSH) access in the RealPresence DMA system security settings, you can log into the RealPresence DMA system remotely as the dmaremote user (for example, dmaremote@<system IP>).

The initial password is !/useResponsibly/!, but you must change this password after the first successful login.

Change the Linux Remote Password

You can change the Linux dmaremote user password for the RealPresence DMA system from the management user interface.

Procedure
1. Go to Admin > Server > Change Linux Remote Password.
2. Complete the password fields as follows:
   • Old password - !/useResponsibly/!
   • New password - Enter the new dmaremote user password.
   • Confirm new password - Re-enter the new password.
3. Click OK.

Usage Data

To continually improve the product, Polycom collects data to understand how customers use the RealPresence DMA system.

By collecting this data, Polycom can identify system level utilization and the combined use of RealPresence DMA system features. This data informs Polycom which features are important and actually used on your system. Polycom uses this information to help guide future development and testing.

Your decision to enable or not enable the sending of this data doesn’t affect the availability of any documented system feature in any way. Enabling this feature doesn’t affect the capacity or responsiveness of the RealPresence DMA system to process calls and conferences, nor does it affect access to the management user interface or API interactions.

The system sends usage data once per hour over a secured (TLS) connection (port 8443) to a Polycom collection point (customerusagedatacollection.polycom.com). There’s no access by any customer or others to view the data received at the collection point. The raw data is viewable only by Polycom. To avoid any impact to starting and ending calls and conferences, data is never sent between 5 minutes before the hour and 5 minutes after the hour.

The following types of data are reported:
• License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, database
- System configuration: number of servers, clusters
- Feature configuration: Enterprise Directory Integration, Skype for Business, Dial Rules, Shared Number Dialing, Hunt Groups, Registration Policy, Device Authentication
- Number of users, endpoints, sites, MCUs, external gatekeepers, SIP peers, SBCs
- Registrations, call and conference statistics
- Security settings

If you enable data collection, your user and environment identifying information (for example, internal IP addresses and FQDNs, names of users, devices, external systems, etc.) is made anonymous before the RealPresence DMA system sends usage data to the data collection point. System serial numbers and license information are sent without anonymization and may be used to help improve customer experiences. In total, less than 100 KB of data per hour is collected and sent.

Polycom's collection and use of this data complies with Polycom's Privacy Policy.

**Enable or Disable Automatic Data Collection**

You can allow or disallow the automatic sending of usage data when you accept the system's end user License Agreement.

The RealPresence DMA system requires HTTPS port 8443 to be open to send usage data.

You can enable or disable this feature at any time.

**Procedure**

1. From the RealPresence DMA management user interface, go to Admin > Server > Licenses.
2. Check or uncheck the Automatically send usage data check box.

**See the Collected Usage Data**

The system records data that has been sent and collected in the system logs.

**Procedure**

1. Log into the RealPresence DMA system as an administrator.
2. Download the system logs.
3. On the PC where the logs have been downloaded, use an archiving or zipping tool to extract the file analytics.json.
   
   analytics.json is a text file containing the hourly data reported most recently before the time when the system logs were created.
4. View the analytics.json file with Notepad or another text editing tool.
Signaling Settings

Topics:

▪ H.323, SIP, and WebRTC Signaling
▪ SIP and H.323 Gateway
▪ Configuring SIP Settings
▪ Configure the SIP Outbound Port Ranges
▪ Configure H.323 Settings
▪ Configure the H.323 Dynamic Port Range
▪ Configure WebRTC Settings
▪ Untrusted SIP Call Handling

The RealPresence DMA system supports H.323, SIP, and WebRTC signaling protocols. Enable at least one protocol for the RealPresence DMA system's conference manager, to receive calls for multipoint conferences, and distribute them among the MCUs configured on the system.

H.323, SIP, and WebRTC Signaling

If H.323 signaling is enabled, the RealPresence DMA system's call server operates as a gatekeeper, receiving registration requests and calls from H.323 devices. If SIP signaling is enabled, the call server operates as a SIP registrar and proxy server, receiving registration requests and calls from SIP devices. If WebRTC signaling is enabled, the call server processes Polycom RealPresence Web Suite conferences initiated from WebRTC-capable web browsers. If you enable more than one signaling protocol, the RealPresence DMA system allows devices using different protocols to communicate in multipoint conferences.

H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster's signaling settings are not changed to match the settings of any other member of the supercluster. To avoid confusion, Polycom recommends that H.323, SIP, and WebRTC signaling settings be configured the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

Note: The settings for untrusted SIP call handling (unauthorized or guest calls) must be the same across all systems in a supercluster.

SIP and H.323 Gateway

The RealPresence DMA system can function as a gateway for point-to-point calls between SIP and H.323 devices, whether they're registered directly to the RealPresence DMA system or to an external device. The gateway function is not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), external addresses, or IP addresses.
As a best practice, Polycom recommends configuring your video conferencing network to avoid using the RealPresence DMA system as a gateway between H.323 and SIP devices.

The gateway functionality doesn’t support the following features:

▪ Media encryption
▪ H.239 content
▪ H.264 high profile content
▪ Dual-tone multi-frequency (DTMF) transmission

Configuring SIP Settings

The RealPresence DMA system supports the use of different ports for private and public network interfaces.

You can configure SIP settings for specific ports for interfaces on both sides of your network.

During installation of a new RealPresence DMA system, the SIP ports 5060 and 5061 are automatically configured with default settings for a core-configured system or an edge-configured system. You can revise the default settings or add new SIP ports if necessary.

The RealPresence DMA system (edge, core, and combination configuration) uses whatever SIP transport type the originator of a call uses to contact a destination. For example, if the call originator uses SIP over UDP, then the RealPresence DMA system connects the call to the destination using SIP over UDP. This means that SIP outbound calls to a remote endpoint on the internet or a VaaS through a RealPresence DMA edge system will use a UDP port if the originating endpoint dialed SIP over UDP. The RealPresence DMA system has no automatic fallback to SIP over TCP if the far end remote endpoint or VaaS does not support SIP over UDP. If TCP/TLS is required, do one of the following:

▪ Configure a SIP peer on the RealPresence DMA edge system with the appropriate transport protocol to connect to the VaaS, enterprise, or service provider you want.
▪ Use SIP peer(s) between the RealPresence DMA core and edge systems with preliminary scripts that set the transport protocol in the SIP URI received from the originating endpoint to the transport protocol that’s needed.

Add a SIP Port

You can configure SIP signaling settings such as ANAT support, as well as device authentication and the default dial plan, Access Control List, and registration policy for specific ports.

Procedure

1. Go to **Service Config > SIP Settings**.
2. Select **Enable SIP signaling**.
3. Select **Enable ANAT support** to enable pass-through of ANAT signaling (RFC 4091 and RFC 4092) in the Session Description Protocol (SDP) for negotiating IP version in a dual-stack (IPv4 + IPv6) environment.
4. Click the **Add** button to add a port and complete the fields as described in the following table:
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port*</td>
<td>The number of the SIP signaling port.</td>
</tr>
<tr>
<td>Transport</td>
<td>Select <strong>TLS</strong> to use the port for encrypted SIP connections. Select <strong>TCP</strong> or <strong>UDP/TCP</strong> to use the port for unencrypted SIP connections. The system answers UDP calls only if that transport type is enabled. For communications back to the endpoint, the system uses the transport protocol that the endpoint requested (provided that the transport is enabled, and for TCP, that unencrypted connections are permitted).</td>
</tr>
<tr>
<td>Network interface</td>
<td>The network interface where the port will be assigned. Select <strong>Private</strong> or <strong>Public</strong>.</td>
</tr>
<tr>
<td>Require mutual authentication</td>
<td>For TLS transport, check this box to enable mutual TLS, requiring callers to present a valid certificate. In <strong>Security Settings</strong>, if the <strong>Allow port level configuration for mutual TLS authentication in the SIP Settings Page</strong> option is unchecked, the system will override the setting here to ensure that mutual TLS certificate validation is always required for security purposes.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong> - The system doesn't issue authentication challenges or check authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authentication</strong> - The system issues authentication challenges and checks authentication credentials for calls to this port. The settings on the <strong>Device Authentication</strong> page determine the realm used for authentication and whether the call server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required) error messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block</strong> - The system blocks calls to this port.</td>
</tr>
<tr>
<td>Dial plan</td>
<td>Select the dial plan the system will use for incoming SIP traffic to this port.</td>
</tr>
<tr>
<td>ACL</td>
<td>Select the Access Control List that will evaluate inbound SIP traffic to this port.</td>
</tr>
<tr>
<td>Registration policy</td>
<td>Select the registration policy to apply to inbound SIP registration requests to this port.</td>
</tr>
</tbody>
</table>

5. **Click OK.**  
6. **Click Update** to save the settings.  
7. **Click Yes** to confirm the updates.

**Edit a SIP Port**

You can revise an individual SIP port’s settings when necessary.
Procedure
1. Go to Service Config > SIP Settings.
2. Select the port to edit and click the Edit button.
3. Revise the fields described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>When selected, enables the port to be used for SIP calls and registrations.</td>
</tr>
<tr>
<td>Port*</td>
<td>The number of the SIP signaling port.</td>
</tr>
<tr>
<td>Transport</td>
<td>Select TLS to use the port for encrypted SIP connections.</td>
</tr>
<tr>
<td></td>
<td>Select TCP or UDP/TCP to use the port for unencrypted SIP connections.</td>
</tr>
<tr>
<td></td>
<td>The system answers UDP calls only if that transport type is enabled.</td>
</tr>
<tr>
<td></td>
<td>For communications back to the endpoint, the system uses the transport</td>
</tr>
<tr>
<td></td>
<td>protocol that the endpoint requested (provided that the transport is</td>
</tr>
<tr>
<td></td>
<td>enabled, and for TCP, that unencrypted connections are permitted).</td>
</tr>
<tr>
<td>Network interface</td>
<td>The network interface where the port is located. Select Private or Public.</td>
</tr>
<tr>
<td>Require mutual authentication</td>
<td>For TLS transport, check this box to enable mutual TLS, requiring callers</td>
</tr>
<tr>
<td>(validation of client certificates)</td>
<td>to present a valid certificate.</td>
</tr>
<tr>
<td></td>
<td>In Security Settings, if the Allow port level configuration for mutual TLS</td>
</tr>
<tr>
<td></td>
<td>authentication in the SIP Settings Page option is unchecked, the system</td>
</tr>
<tr>
<td></td>
<td>will override the setting here to ensure that mutual TLS certificate</td>
</tr>
<tr>
<td></td>
<td>validation is always required for security purposes.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>▪ None - The system doesn't issue authentication challenges or check</td>
</tr>
<tr>
<td></td>
<td>authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>▪ Authentication - The system issues authentication challenges and checks</td>
</tr>
<tr>
<td></td>
<td>authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>The settings on the Device Authentication page determine the realm used</td>
</tr>
<tr>
<td></td>
<td>for authentication and whether the call server responds to unauthenticated</td>
</tr>
<tr>
<td></td>
<td>requests with 401 (Unauthorized) or 407 (Proxy Authentication Required)</td>
</tr>
<tr>
<td></td>
<td>error messages.</td>
</tr>
<tr>
<td></td>
<td>▪ Block - The system blocks calls to this port.</td>
</tr>
<tr>
<td>Dial plan</td>
<td>Select the dial plan the system will use for incoming SIP traffic to this</td>
</tr>
<tr>
<td>ACL</td>
<td>Select the Access Control List that will evaluate inbound SIP traffic to</td>
</tr>
<tr>
<td>Registration policy</td>
<td>Select the registration policy to apply to inbound SIP registration requests to this port.</td>
</tr>
</tbody>
</table>
4. Click OK.
5. Click Update to save the settings.
6. Click Yes to confirm the updates.

Delete a SIP Port
You can delete a SIP port when it's not in use.

Procedure
1. Go to Service Config > SIP Settings.
2. Select the port to delete and click the Delete button.
3. Click Yes to confirm the deletion.
4. Click Update to save the settings.
5. Click Yes to confirm the updates.

Configure the SIP Outbound Port Ranges
You can configure the range of outbound ports for SIP signaling services.

The total ports required for each call may vary based on the signaling negotiations used to set up the call. The default SIP port range provides the best balance between maximum calls the RealPresence DMA system can support, and the required number of open firewall ports. Reducing the range may limit the maximum number of calls for which the system can provide SIP signaling services; apply caution if changing the range is necessary.

Caution: The specific ports and port ranges you configure in the RealPresence DMA system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

The following table summarizes outbound port information for SIP signaling services.

<table>
<thead>
<tr>
<th>Service</th>
<th>First Port</th>
<th>Last Port</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP outbound ports (private)</td>
<td>13001</td>
<td>23000</td>
<td>The network interfaces on the private side with SIP signaling services assigned.</td>
</tr>
<tr>
<td>SIP outbound ports (public)</td>
<td>13001</td>
<td>23000</td>
<td>The network interfaces on the public side with SIP signaling services assigned.</td>
</tr>
</tbody>
</table>

If you change the port range settings, the RealPresence DMA system validates the new settings to ensure that no overlap occurs among any of the port range settings for RealPresence DMA system services. Additionally, the system checks the port ranges to confirm the following:

- No first port number is less than 1024.
- No last port number is greater than 65535.

Procedure
1. Go to Service Config > SIP Settings.
2. Click Port Range Settings.
3. For SIP outbound ports (private), enter the First Port and Last Port numbers of the port range.
4. For **SIP outbound ports (public)**, enter the **First Port** and **Last Port** numbers of the port range.
5. Click **OK**.
6. Click **Yes** to confirm the settings.

### Restore the Default SIP Ports

If you change the default SIP ports, you can restore the defaults if necessary.

**Procedure**

1. Go to **Service Config > SIP Settings**.
2. Click **Port Range Settings**.
3. Click **Restore Defaults**.
4. Click **Update** to restore the default settings.
5. Click **Yes** to confirm the action.

### Configure H.323 Settings

The RealPresence DMA system supports the use of different ports for LAN (private) and WAN (public) network interfaces.

You can configure H.323 settings for interfaces on both sides.

You can configure H.323 signaling settings such as ports used, multicast, as well as device authentication and the default dial plan, Access Control List, and registration policy for LAN and WAN side interfaces.

**Procedure**

1. Go to **Admin > Server > H.323 Settings**.
2. Select **Enable H.323 signaling**.
3. For **Policy Selection**, choose one of the following:
   - By port number
   - By topology
4. Enter the port numbers for the **H.225 port** and **RAS port**.
   - It's recommended that you keep the default port numbers (1720 for H.225 port, 1719 for RAS port).
5. Select a **Dial plan** from the drop-down list.
6. Select an **ACL** from the drop-down list.
   - **Factory Core ACL** is the default Access Control List (ACL) for core-configured systems.
   - **Factory Edge ACL** is the default ACL for edge-configured systems.
7. Select a **Registration policy** from the drop-down list.
   - **Factory Core Registration Policy** is the default registration policy for core-configured systems.
   - **Factory Edge Registration Policy** is the default registration policy for edge-configured systems.
8. Select **H.323 multicast** to support gatekeeper discovery messages from endpoints.
9. Select **Enable H.323 device authentication** to turn on H.235 authentication.
   - You must add device authentication credentials for **Inbound Device Authentication** in the **Device Authentication** settings.
10. Select **Enable H.460 NAT traversal** to enable firewall traversal support.
11. Enter the H.460 external client registration interval, which is the number of seconds between a client's lightweight registrations to the gatekeeper.
12. Click Update to save your settings.

**Configure the H.323 Dynamic Port Range**

You can configure the dynamic port range for H.323 signaling services. The total ports required for each call may vary based on the signaling negotiations used to set up the call.

The default H.323 port range provides the best balance between maximum calls the RealPresence DMA system can support, and the required number of open firewall ports. Reducing the range may limit the maximum number of calls for which the system can provide H.323 signaling services; apply caution if changing the range is necessary.

**Caution:** The specific ports and port ranges you configure in the RealPresence DMA system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

The following table summarizes dynamic port information for H.323 signaling services.

<table>
<thead>
<tr>
<th>Service</th>
<th>First Port</th>
<th>Last Port</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 dynamic ports (H.245)</td>
<td>35001</td>
<td>40000</td>
<td>The network interfaces with H.323 signaling services assigned.</td>
</tr>
</tbody>
</table>

If you change the port range settings, the RealPresence DMA system validates the new settings to ensure that no overlap occurs among any of the port range settings for RealPresence DMA system services. Additionally, the system checks the port ranges to confirm the following:

- No first port number is less than 1024
- No last port number is greater than 65535

**Procedure**

1. Go to Service Config > H323 Settings.
2. Click Port Range Settings.
3. For H.323 dynamic ports, enter the First Port and Last Port numbers of the port range.
4. Click OK.
5. Click Yes to confirm the settings.

**Restore the Default H.323 Ports**

If you change the default H.323 dynamic port range, you can restore the default range if necessary.

**Procedure**

1. Go to Service Config > H.323 Settings.
2. Click Port Range Settings.
3. Click Restore Defaults.
4. Click Update to restore the default settings.
5. Click Yes to confirm the action.
Configure WebRTC Settings

You can enable WebRTC signaling in a RealPresence DMA core-configured system if you have WebRTC clients on your network.

WebRTC signaling should be enabled if you have a RealPresence DMA edge-configured system that provides TURN services.

H.323, SIP, and WebRTC signaling settings are specific to an individual cluster. When you add a cluster to a supercluster, the cluster’s signaling settings are not changed to match the settings of any other member of the supercluster. It’s recommended that you configure all H.323, SIP, and WebRTC signaling settings to be the same across all clusters in a supercluster, except when a specific deployment requires them to be different.

Procedure

1. Go to Admin > Server > WebRTC Settings.
2. Select Enable WebRTC signaling.
3. Select a Dial plan from the drop-down list.
4. Click Update to save your settings.

Untrusted SIP Call Handling

You can configure special handling for SIP calls from devices outside the corporate firewall that are not registered with the RealPresence DMA system and are not from a federated division or enterprise.

These calls come to the RealPresence DMA system via session border controllers (SBCs) such as a RealPresence DMA Access Director system or Acme Packet Session Border Controller (which are configured as external SIP peers in the RealPresence DMA system).

You can route such untrusted (unauthorized or guest) calls by creating a separate set of guest dial rules used only for these untrusted calls.

You can add one or more ports so that an SBC can route untrusted calls to a specific port. For each port, you can specify whether authentication is required. You can also specify the transport, and if TLS, whether certificate validation is required (mutual TLS).

Although these are cluster-specific settings that are not part of the data store shared across superclustered systems, we strongly recommend that all signaling settings be the same across all clusters in a supercluster.

The settings for untrusted SIP call handling (unauthorized or guest calls) must be the same across all clusters in a supercluster.

If you add ports for untrusted calls, you must also create and associate a dial plan for those calls.

Guest Ports

You can maintain a list of external ports for guest users and customize the SIP settings for each, including dial plans and authentication settings.

Add a New Guest Port

You can add a port to the RealPresence DMA system to be used for SIP guest calls.
Procedure
1. Go to Service Config > SIP Settings.
2. Under Unauthorized ports, click the Add button.
3. Configure the parameters for the guest port.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>When selected, enables the port to be used for guest SIP calls.</td>
</tr>
<tr>
<td>Port</td>
<td>The number of the SIP signaling port.</td>
</tr>
<tr>
<td></td>
<td>This is the port number that a session border controller is configured to use for guest (untrusted) calls to the RealPresence DMA system via the transport specified below.</td>
</tr>
<tr>
<td>Transport</td>
<td>To use this guest port for unencrypted SIP connections, select either TCP or UDP/TCP from the list. To use this port for encrypted SIP connections, select TLS.</td>
</tr>
<tr>
<td>Require mutual authentication</td>
<td>For TLS transport, check this box to enable mutual TLS, requiring callers to present a valid certificate.</td>
</tr>
<tr>
<td>(validation of client certificates)</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>▪ None - The system doesn't issue authentication challenges or check authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>▪ Authentication - The system issues authentication challenges and checks authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>The settings on the Device Authentication page determine the realm used for authentication and whether the call server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required).</td>
</tr>
<tr>
<td></td>
<td>▪ Block - The system blocks calls to this port.</td>
</tr>
<tr>
<td>Dial plan</td>
<td>Select a dial plan to use for this port.</td>
</tr>
</tbody>
</table>

4. Click OK.

Edit a Guest Port
You can edit a guest port that you've added to the RealPresence DMA system SIP Settings when necessary.

Procedure
1. Go to Service Config > SIP Settings.
2. Under Unauthorized ports, select the port to edit and click the Edit button.
3. Revise the following parameters for the guest port as needed:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>When selected, enables the port to be used for guest SIP calls.</td>
</tr>
<tr>
<td>Port</td>
<td>The number of the SIP signaling port.</td>
</tr>
<tr>
<td></td>
<td>This is the port number that a session border controller is configured to use for guest (untrusted) calls to the RealPresence DMA system via the transport specified below.</td>
</tr>
<tr>
<td>Transport</td>
<td>To use this guest port for unencrypted SIP connections, select either TCP or UDP/TCP from the list. To use this port for encrypted SIP connections, select TLS.</td>
</tr>
<tr>
<td>Require mutual authentication</td>
<td>For TLS transport, check this box to enable mutual TLS, requiring callers to present a valid certificate.</td>
</tr>
<tr>
<td>(validation of client certificates)</td>
<td><strong>Note:</strong> If the Allow port level configuration for mutual TLS authentication in the SIP Settings Page option is unchecked in Security Settings, the system will override the setting here to ensure that mutual TLS certificate validation is always required for security purposes.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• None - The system doesn’t issue authentication challenges or check authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>• Authentication - The system issues authentication challenges and checks authentication credentials for calls to this port.</td>
</tr>
<tr>
<td></td>
<td>The settings on the Device Authentication page determine the realm used for authentication and whether the call server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required).</td>
</tr>
<tr>
<td></td>
<td>• Block - The system blocks calls to this port.</td>
</tr>
<tr>
<td>Dial plan</td>
<td>Select a dial plan to use for this port.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Dial Rules for Guest Calls**

If you enabled the system to receive unauthorized or guest calls, you also need to configure specific dial rules to route the unauthorized or guest calls.

The system comes with a default Guest Dial Plan to which you can add dial rules. Alternatively, you can create your own dial plan with a different name.

**Add a Dial Rule for Guest Calls**

You can add one or more dial rules to route unauthorized calls.

A preliminary is an executable script, written in the JavaScript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule’s action is performed.
Procedure

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select Guest Dial Plan.
3. Click the Add Dial Rule button.
4. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text description that will display under Dial Rules-Guest Dial Plan on</td>
</tr>
<tr>
<td></td>
<td>the Dial Plans page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed on unauthorized calls. When you select some</td>
</tr>
<tr>
<td></td>
<td>actions, additional settings become available.</td>
</tr>
</tbody>
</table>

5. Click OK.

Edit a Dial Rule for Guest Calls

Dial rules for guest calls specify how to route unauthorized calls.

You can edit these dial rules as needed.

Procedure

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select Guest Dial Plan.
3. Select the dial rule to edit and click the Edit Dial Rule button.
4. Revise the fields as described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The text description that will display under Dial Rules-Guest Dial Plan on</td>
</tr>
<tr>
<td></td>
<td>the Dial Plans page.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to be performed on unauthorized calls. When you select some</td>
</tr>
<tr>
<td></td>
<td>actions, additional settings become available.</td>
</tr>
</tbody>
</table>
**Primary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>When checked, the preliminary script is active.</td>
</tr>
<tr>
<td></td>
<td>When cleared, the preliminary script is turned off but not deleted.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the preliminary script to apply to the dial string.</td>
</tr>
<tr>
<td>Debug this Script</td>
<td>Click to debug (test) the preliminary script with different variables.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
Two core-configured or two edge-configured RealPresence DMA systems can be set up on the same network to provide High Availability (HA) of services. Systems configured for HA support minimal interruption of services and greater call reliability.

The RealPresence DMA system supports two HA configurations:

- **Active-passive** - The two RealPresence DMA systems share one set of virtual IP addresses for each enabled network interface with services assigned. If one system fails, the peer system takes over the failed system's resources (virtual IP addresses and assigned services). All active calls are either dropped automatically or callers must manually hang up, but registration and provisioning information for endpoints is maintained in memory and shared between both systems. Once all resources are re-established on the peer system, users can call back in to the video conference without changing any call information.

- **Active-active** - Each RealPresence DMA system has virtual IP addresses for each enabled network interface with services assigned. Both systems run concurrently and load balancing occurs between the two systems. This configuration increases throughput for media, making use of both systems so you have full capacity.

**Note:** An active-active HA pair can’t be part of a supercluster.

### Failovers

After HA is enabled and configured, the two RealPresence DMA systems communicate status by sending each other messages via the network interfaces configured as HA links.

If communication between the two systems is disrupted, a failover may occur:

- If the standby (active/passive) or peer (active/active) does not receive a response for an ARP ping of all VIPs (active/passive) or all the peer's VIPs (active/active) then the standby or peer will attempt to take over all VIPs (active/passive) or all the peer's VIPs (active/active).

- During a failover, the system that is operating correctly takes over the resources (VIPs and the associated services) of the system that failed.

- A system failover typically requires 10 to 30 seconds for all resources to be available on the peer system.
When an active/active system that failed is running again, it requests its original resources back from the peer system. If the peer system doesn’t have any active calls, it releases the resources back to the system that previously failed.

When an active/passive system that failed is running again, it becomes the standby system.

The following situations will cause a failover to occur or not occur:

- A server fails
- All HA links fail (if at least one HA link is running normally, a failover won’t occur)
- If all HA links fail but the VIPs are still active, a failover won’t occur
- A network interface with a VIP fails (if more than one NIC has a VIP, all resources will be taken over, not just those associated with the failed NIC)

Network Settings to Support High Availability

When you configure the network settings for your two RealPresence DMA systems, consider the following information:

- Network requirements between the two RealPresence DMA systems: 100 Mbps link and less than 200 ms delay.
- The RealPresence DMA system supports the use of multiple network interfaces, which can be physical network interface cards (NIC), virtualized NICs (if using Virtual Edition), or RealPresence DMA logical network interfaces such as LACP (bonded) and VLAN (see Network Settings).
- Determine the number of interfaces your network configuration needs and identify the interfaces to use for RealPresence DMA services, dedicate exclusively to HA messaging, or use for both purposes.
- Assign static IP addresses to all interfaces on both nodes in the HA pair that will be used as HA links or that have services assigned. Each node must use the same interface for the same purpose (for example, if eth0 has all services assigned to it on node A, then eth0 on node B should have all services assigned; if bond0 is an HA link on node A, it must also be an HA link on node B). Each network interface on node A must be on the same subnet as the corresponding interface on node B.
- A network interface with services assigned may also be used for HA communication
- At a minimum, configure at least one network interface for RealPresence DMA services (for example, call signaling, administrative management) and one network interface (possibly the same one) for HA messaging between the two RealPresence DMA nodes.
- Configure the network settings for all of the network interfaces you plan to use on each system before you enable HA and configure its settings. Once HA is enabled, configuring network settings is disabled.
- If you deploy the systems behind a firewall and your network requires a NAT address, map the NAT address to the virtual IP address rather than the physical address for each interface that has assigned public signaling services and public media traversal services.

The physical IP addresses of the same network interfaces on each system (for example, eth1 and eth1) must be on the same subnet.

- Assign the same services to the same network interfaces on each system.
- Network interfaces assigned to media traffic should not be used as HA links.
- If you plan to configure one or more network interfaces as dedicated HA links (no assigned services), you need to assign IP addresses based on the physical location of your two RealPresence DMA systems:
If the two systems are located physically close to each other and the direct link cable doesn’t need to be routed within your network, the IP addresses you assign to the dedicated HA interfaces don’t need to be within your network IP space but they must be on the same subnet.

If your two systems aren’t located in the same area, the IP addresses you assign to the dedicated HA interfaces must be within your network IP space and on the same subnet.

High Availability Requirements

When you configure your HA settings, follow these requirements:

▪ Configure all other settings for the RealPresence DMA system identically on both systems.

▪ Configure one virtual IP address for each network interface that has assigned services. If both IPV4 and IPV6 are enabled, configure one virtual IPv4 and one virtual IPV6 address.
  • A virtual IP address must be on the same subnet as the physical IP address for the network interface.
  • Use only IP addresses that are not already in use. The RealPresence DMA system doesn’t prevent IP address conflicts and, if they occur, your HA systems won’t operate correctly.

▪ Configure at least one network interface to be used for HA traffic (an HA link). The HA link can be a LAN connection to the physical IP address of the same NIC on the peer system or it can be a direct (crossover) link. A direct link physically connects two network interfaces on a private network. Use one or both of the following settings to configure an HA link:
  • **Enable Interface for HA traffic**: When enabled, the network interface can act as a dedicated HA link or it can also have assigned services. If you select this option, you must provide the physical IP address of the same NIC on the peer system.
  • **Use Direct Link**: When enabled, the network interface acts as a private network HA link and can’t have assigned services. Don’t assign a virtual IP address to a direct link.

▪ Multiple HA links are not supported if they are on the same subnet.

▪ HA messaging traffic must be routable if the systems don’t have a direct link.

▪ If you upgrade from the RealPresence Access Director system, you need to transition existing media IP addresses to virtual IP addresses and assign new IP addresses to the physical interfaces. This will prevent you from having to change IP addresses on your firewall.

Configure High Availability Settings

Virtual HA settings are required only for network interfaces with assigned services.

Direct links can’t have services assigned and don’t require virtual IP addresses. Virtual IP addresses are tied to services but HA only communicates via physical IP addresses.

When you configure HA settings for the first time on one RealPresence DMA system, some of that system’s configuration settings will be shared when you configure the peer system. After the initial configuration, changes on one system will automatically be updated to the other system. Settings that are unique to one system (for example, network configuration, network name, call history) are not shared.

Virtual addresses remain inactive until both nodes have been configured.
Note: When you configure HA Interface Settings, you need to enter the required information for each active NIC before you submit your HA settings. If you try to submit partial settings, errors may result from missing information.

Procedure

1. Go to Admin > Server > High Availability Settings.
2. Use the information in the following table to configure the HA settings for your system.

### General HA

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable high availability (HA)</td>
<td>When selected, enables HA.</td>
</tr>
<tr>
<td>HA mode</td>
<td>Active:Passive</td>
</tr>
<tr>
<td></td>
<td>Active:Active</td>
</tr>
</tbody>
</table>

### HA Link Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface (eth0, eth1, eth2, eth3)</td>
<td>Lists the physical IP address of each network interface on your local system. If multiple local physical addresses are present (IPv4 and IPv6), select one address from the drop-down menu.</td>
</tr>
<tr>
<td></td>
<td>HA traffic - When selected, the interface is used for HA traffic and communicates with the peer system via the Peer physical IP address for the same network interface. Note that you shouldn’t enable HA traffic for more than one interface on the same subnet.</td>
</tr>
<tr>
<td></td>
<td>Direct link - When selected, the interface must have a direct, physical link (crossover or Ethernet cable) to the same network interface on the peer system. You must enter the Peer physical IP but you don't need to specify a virtual IP address for the interface. Recommended setting if your two HA systems are co-located. Direct link interfaces cannot have services assigned.</td>
</tr>
<tr>
<td></td>
<td>Peer physical IP - If the network interface is used for HA traffic, you must provide the physical IP address of the peer system. The peer physical address needs to be the same address type (IPv4/ IPv6) as the local physical address.</td>
</tr>
</tbody>
</table>
## HA Interface Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name, IP address, and CIDR of each network interface (eth0, eth1, eth2, eth3)</td>
<td>The name of each interface that is eligible for HA configuration displays with its physical address (IPv4/IPv6) and its associated CIDR mask. Disabled network interfaces display but cannot be assigned HA settings.</td>
</tr>
<tr>
<td>Configured services</td>
<td>When you hover over the text, the system services assigned to the network interface display.</td>
</tr>
<tr>
<td>Local virtual IPv4/IPv6</td>
<td>The virtual IP address of the network interface on your local system. Use only an IP address that is not already in use. The RealPresence DMA system doesn’t prevent IP address conflicts and, if they occur, your HA systems won’t operate correctly. The local physical IP address, <strong>Local Virtual IP IPv4/IPv6</strong>, and <strong>Peer Virtual IP IPv4/IPv6</strong> must be on the same subnet for the selected interface. If the network interface has assigned services, the virtual IP address will inherit the same service bindings.</td>
</tr>
<tr>
<td>Local virtual hostname</td>
<td>Virtual hostname of the network interface on your local system. Required only on network interfaces with assigned services. Example: <strong>ha-dma-1-0</strong> A hostname can contain the following characters: a-z A-Z 0-9 - . (periods are allowed only in domain style names) Blank spaces and underscores are not allowed.</td>
</tr>
<tr>
<td>Peer virtual IPv4/IPv6</td>
<td>The virtual IP address for the same interface on the peer system. Required for <strong>Active:Active</strong> only.</td>
</tr>
</tbody>
</table>
3. **Select the HA traffic** check box to indicate the network interfaces that will be used for HA communication between the two systems.

4. **Click Submit.**
   The system reboots.

5. **After the local system restarts, go to Admin > High Availability Settings.**

6. **Click Configure Peer** to apply the same HA settings to the peer system.
   This step is required to configure the peer system.

7. **Complete the following fields (all are required):**
   - **Peer management IP address** - Enter the management IP address of the peer system.
   - **Peer Port** - Port 8443 is the default port for the peer system.
   - **Peer Admin Account** - The username that the peer system administrator uses to log in to the system's web user interface.
   - **Peer Admin Password** - The peer system administrator's login password.
   - Click **OK**. The selected peer reboots and will be configured with the HA settings from your local system. After the peer system reboots and the user interface login screen displays, you may not be able to log in for several minutes until the database is completely synchronized.

---

**Regenerate a High Availability Encryption Key**

When you configure two RealPresence DMA systems for HA, the two systems share an internal encryption key that supports secure communication between the systems.

Changing the encryption key is typically not necessary, however, this option provides the ability to comply with strict security policies.

**Caution:** Change the HA encryption key only when both systems have no active calls. Otherwise, all active calls will be dropped when you submit the changes from the High Availability Settings page.
Procedure

1. Go to Admin > Server > High Availability Settings.
2. Select Regenerate HA encryption key.
3. Click Submit.
   The system reboots.
4. After the system restarts, go to Admin > Server > High Availability Settings.
5. Click Configure Peer.
6. Enter the name and password and click OK.
   The peer system reconnects and all HA settings are applied to the peer system, including the new HA encryption key.

Licensing Calls for High Availability Systems

It's recommended that you license each server or allocate each virtual instance with the same number of calls.

For instructions on licensing your RealPresence DMA systems, see Licensing in the Polycom RealPresence DMA Administrator Guide.

Certificates for High Availability Systems

When you deploy two new RealPresence DMA systems for HA, each system has a default self-signed SSL certificate.

To ensure that both of your systems are identified as trusted entities, it's recommended that you request signed identity certificates from a certificate authority (CA). Each RealPresence DMA system should have a signed certificate that includes the following information in its subject alternative name (SAN) or common name (CN) fields:

- FQDNs for the physical hostnames and virtual hostnames

It's recommended that you add IP addresses and physical hostnames and virtual hostnames (without the domain) as SANs.

After you receive the signed certificates, you need to add (install) them on both RealPresence DMA systems after you enable and configure network and HA settings. Additionally, you need to install your chosen CA's public certificate on each system.

Note that when you enable HA, the system checks the certificate to determine if the minimum requirements for SANs have been met and will regenerate a self-signed certificate only if the required information cannot be found. If you upgrade your HA systems to a new version of the RealPresence DMA software, each system will regenerate a self-signed certificate only if the existing certificate is self-signed.

If you disable HA at any time, the certificates on the two systems remain intact.

If you accidentally delete a signed certificate, you can restore it from a system backup file or create a certificate signing request (CSR) for a new signed certificate.
**Note:** When you make changes to the RealPresence DMA system, it will cause a new certificate to be generated, or when you install a new certificate, you may need to refresh or reload your browser before you log back into the management user interface. If you refresh your browser and still see outdated information or cannot download log files in the RealPresence DMA system, you need to clear your browser’s cache.

---

**Integrating High Availability Systems with the RealPresence Resource Manager System**

If you plan to integrate your RealPresence DMA High Availability systems with a RealPresence Resource Manager system, configure the network settings on both HA nodes and enable and configure the HA settings **before** you integrate with the RealPresence Resource Manager system.

After the systems are integrated, you need to create three entries in the RealPresence Resource Manager system for the RealPresence DMA system HA pair as follows:

- For an active-passive configuration, one entry must point the RealPresence Resource Manager system to the virtual IP address of the management interface to integrate network and site topology information. For an active-active configuration, the entry can point the RealPresence Resource Manager system to the virtual IP address of the management interface on either of the two nodes.

- Two entries must point the RealPresence Resource Manager system to the physical IP address of the management interface for each system in the HA pair to obtain license information in a Polycom RealPresence Clariti environment.

**DNS Records for High Availability**

Your RealPresence Resource systems must be accessible by their host name(s), not just their IP address(es), so you (or your DNS administrator) must create the necessary A (and/or AAAA) records, as well as the corresponding PTR records, on your DNS server(s).

A (IPv4) and AAAA (IPv6) records map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address. The corresponding PTR records allow reverse DNS resolution of the system’s physical or virtual host name(s).

Depending on local DNS configuration, a host name could be the RealPresence Resource system’s fully qualified domain name (FQDN) or a shorter name that DNS can resolve.
Security Settings

Topics:

- Selecting a Security Mode

The RealPresence DMA system security settings enable you to switch between enhanced security mode and a custom security mode, in which you can enable one or more insecure network access capabilities. Polycom recommends that you use the enhanced security mode unless you have a specific need to allow one of the insecure capabilities.

Selecting a Security Mode

When you select Enhanced security mode, all Custom security mode options are unchecked and disabled.

You can still configure some settings that can be applied to either security mode.

When you select Custom security mode, all custom options are unchecked by default. You can then select the specific capabilities you need for network access to your RealPresence DMA system environment.

Whether you use enhanced or custom security mode, your settings are not locked and the ability to lock settings isn’t supported. You can switch to the other security mode when necessary for your environment.

Note: All systems in a supercluster must have the same security settings. If you invite a system to join an existing supercluster, the invited system's security settings will be changed to match those of the supercluster. You can’t change a system's security settings while it’s part of a supercluster.

Configure Security Settings

When you configure security settings, you can select the system's security level and configure various network access settings.

If you enable Secure Shell (SSH) access, when a user logs in to the RealPresence DMA system by SSH, access is provided only through the interface you selected for management in the Services settings for your network.

If a problem occurs with the RealPresence DMA system that causes it to crash or not boot up correctly, SSH access is enabled automatically for the management interface. This way, when you contact Polycom Global Services for assistance, a Polycom support technician, with your permission and access to your network, can access your RealPresence DMA system with SSH and troubleshoot the issue.

Caution: If you select SSL 3.0 as a security protocol for HTTPS communication, but don’t select at least one TLS protocol (TLS 1.0, TLS 1.1, or TLS 1.2), you may not be able to access the RealPresence DMA system web interface in most browsers. It’s recommended that you select at least one TLS protocol.

Procedure

1. Go to Admin > Server > Security Settings.
2. Select the security settings needed for your system as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced security</td>
<td>When selected, this mode disables all <strong>Custom security options</strong> (unencrypted protocols and non-essential system access methods).</td>
</tr>
<tr>
<td>Custom security</td>
<td>When selected, this mode enables you to select one or more of the unsecured methods of network access listed in the check boxes.</td>
</tr>
<tr>
<td>Allow console access</td>
<td>When selected, enables the root user to log into the system via a console. Default: Enabled for core configuration and edge configuration.</td>
</tr>
<tr>
<td>Allow SSH root user access</td>
<td>When selected, enables SSH access to the system and the root user may log into the shell. This bypasses the need to log in as the dmaremote user first, although that user may also log in anytime SSH access is available. Default: Enabled for core configuration, disabled for edge configuration.</td>
</tr>
<tr>
<td>Allow SSH access</td>
<td>When selected, SSH is enabled and the dmaremote user (for example, dmaremote@&lt;system IP&gt;) may log into the system. The initial password is <em>/useResponsibly/</em>, and the user will be forced to change this after the first successful login. The dmaremote user runs in a restricted shell and many shell commands are not available. The dmaremote user needs to escalate (su) to the root user to perform any major system operations from the command line. Default: Enabled for core configuration, disabled for edge configuration.</td>
</tr>
<tr>
<td>Allow unencrypted connections to the Active Directory</td>
<td>The RealPresence DMA system connects to Active Directory using SSL or TLS encryption. However, if the Active Directory server or servers (including domain controllers if you import global groups) are not configured to support encryption, the RealPresence DMA system can only connect using an unencrypted protocol. This option allows such connections if an encrypted connection cannot be established. When selected, the unencrypted passwords of enterprise users are transmitted over the network. Use this option only for diagnostic purposes. By toggling it, you can determine whether encryption is the cause of a failure to connect to Active Directory or to load group data. If so, the solution is to correctly configure the relevant servers, not to allow ongoing use of unencrypted connections.</td>
</tr>
<tr>
<td>Allow unencrypted connections to MCUs</td>
<td>The RealPresence DMA system uses only HTTPS for the conference control connection to RealPresence Collaboration Server or RMX MCUs, and therefore can’t control an MCU that accepts only HTTP (the default). This option enables the system to fall back to HTTP for MCUs not configured for HTTPS. Polycom recommends configuring your MCUs to accept encrypted connections rather than enabling this option. When unencrypted connections are used, the RealPresence Collaboration Server or RMX login name and password are sent unencrypted over the network.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Allow unencrypted calendar notifications from Exchange server | If calendaring is enabled, the RealPresence DMA system gives the Microsoft Exchange server an HTTPS URL to which the Exchange server can deliver calendar notifications. The RealPresence DMA system must have a certificate that the Exchange server accepts in order for the HTTPS connection to work.  
If this option is selected, the RealPresence DMA system provides an HTTP URL, which the Exchange server uses to send calendar notifications.  
Polycom recommends installing a certificate trusted by the Exchange server and using an HTTPS URL for notifications rather than enabling this option. |
| Allow basic authentication to Exchange server               | If calendaring is enabled, the RealPresence DMA system authenticates itself with the Exchange server using NTLM authentication.  
If this option is selected, the RealPresence DMA system still attempts to use NTLM first, but if it fails or isn’t enabled on the Exchange server, then the RealPresence DMA system falls back to HTTP Basic authentication (user name and password).  
Polycom recommends using NTLM authentication rather than enabling this option.  
For either NTLM or HTTP Basic authentication to work, they must be enabled on the Exchange server. |
| Allow port level configuration for mutual TLS authentication in the SIP Settings Page | During encrypted call signaling (SIP over TLS), the RealPresence DMA system requires the remote party (endpoint or MCU) to present a valid certificate. This is known as mutual TLS.  
When selected, the port level configuration will be used rather than having the RealPresence DMA system always require mutual TLS when endpoints are signaling over TLS.  
Polycom recommends installing valid certificates on your endpoints and MCUs rather than enabling this option. |
| Allow third-party applications to receive SIP RFC 4575 conference events | The SIP SUBSCRIBE/NOTIFY conference notification service (as described in RFCs 3265 and 4575), allows SIP devices to subscribe to a conference and receive conference rosters and notifications of conference events. Normally, the subscribing endpoints are conference participants.  
This option configures the system to let devices subscribe to a conference without being participants in the conference.  
**Note:** A subscription to a conference by a non-participant consumes a call license. Call history doesn’t include data for non-participant subscriptions. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use non-FIPS mode (change will cause system restart)</td>
<td>When selected, non-FIPS-compliant protocols and access methods are supported. Federal Information Processing Standards (FIPS) are standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. The standards establish requirements for various purposes, such as ensuring computer security and interoperability, and are intended for cases in which suitable industry standards do not already exist. When the check box is cleared, the system uses FIPS mode and the <strong>Skip validation of certificates received while making outbound connections</strong> check box is automatically cleared and disabled. When in FIPS mode, validation of certificates is mandatory.</td>
</tr>
<tr>
<td>Skip validation of certificates received while making outbound connections</td>
<td>When the RealPresence DMA system connects to a server, it validates that server's certificate. This option configures the system to accept any certificate presented to it without validating it. Polycom recommends using valid certificates for all servers that the system may need to contact rather than enabling this option. Depending on system configuration, this may include: • MCUs • Active Directory • Exchange • RealPresence DMA system • Other RealPresence DMA systems • Endpoints <strong>Note:</strong> Either the common name (CN) or subject alternative name (SAN) field of the server's certificate must contain the address or host name that the RealPresence DMA system specifies for that server. For example, if the RealPresence DMA system is integrated with an Active Directory system with the FQDN <code>DC.myenterprise.com</code>, then the RealPresence DMA system will validate that the certificate it receives has either a CN or SAN entry for <code>DC.myenterprise.com</code>. Polycom MCUs do not include their management IP address in the SAN field of the certificate signing request (CSR), so their certificates identify them only by the CN. Therefore, in the RealPresence DMA system, an MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by IP address. Similarly, an Active Directory server certificate often specifies only the FQDN. So in the RealPresence DMA system, identify the enterprise directory by FQDN, not by IP address.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow system booting from USB or optical drive (does not apply to RealPresence DMA Virtual Edition) (change will cause system restart)</td>
<td>When selected, the system can be booted from a USB device or an optical drive. If this check box is cleared, the boot order is configured so that the server cannot be booted from a USB device or the optical drive.</td>
</tr>
<tr>
<td>Require endpoints to be provisioned for LDAP and XMPP access</td>
<td>When selected, endpoints must be provisioned before they can access LDAP and XMPP services.</td>
</tr>
<tr>
<td>Allow non-TLS connections through access proxy to LDAP</td>
<td>When selected, non-TLS LDAP requests that come through access proxy are allowed access to LDAP services.</td>
</tr>
</tbody>
</table>

**The following settings may be configured in any security mode**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip validation of certificates for inbound connections</td>
<td>This option affects inbound connections from entities like web browsers and API clients.</td>
</tr>
<tr>
<td></td>
<td>If this check box is cleared, you can only connect to the RealPresence DMA system if your browser presents a client certificate issued by a CA that the system trusts (this is known as mutual TLS for administrative connections).</td>
</tr>
<tr>
<td></td>
<td>Clear this check box only if:</td>
</tr>
<tr>
<td></td>
<td>• You have implemented a complete public key infrastructure (PKI) system, including a CA server, client software (and optionally hardware, tokens, or smartcards), and the appropriate operational procedures.</td>
</tr>
<tr>
<td></td>
<td>• The CA’s public certificate is installed in the RealPresence DMA system so that it trusts the CA.</td>
</tr>
<tr>
<td></td>
<td>• All authorized users, including yourself, have a client certificate signed by the CA that authenticates them to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Allow forwarding of IPv6 ICMP destination unreachable messages</td>
<td>When this check box is cleared, the RealPresence DMA system has an internal firewall rule that blocks outbound destination unreachable messages.</td>
</tr>
<tr>
<td></td>
<td>When selected, the internal firewall rule is disabled.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system currently does not send such messages, regardless of this setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The RealPresence DMA system currently does not send such messages, regardless of this setting.</td>
</tr>
<tr>
<td>Allow IPv6 ICMP echo reply messages to multicast addresses</td>
<td>When this check box is cleared, the RealPresence DMA system does not reply to echo request messages sent to multicast addresses (multicast pings).</td>
</tr>
<tr>
<td></td>
<td>When selected, the system responds to multicast pings.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore SIP <strong>critical</strong> privacy flag</td>
<td>When selected, the RealPresence DMA system ignores the <strong>critical</strong> flag in the Privacy header of incoming SIP messages, and accepts calls marked with this flag. When this check box is cleared, the system rejects incoming calls that include a <strong>critical</strong> flag in the Privacy header and sends a 500 response code.</td>
</tr>
<tr>
<td>Remove <strong>critical</strong> flag</td>
<td>If you select the Ignore SIP <strong>critical</strong> privacy flag check box, this option (when selected) instructs the RealPresence DMA system to remove the <strong>critical</strong> flag from the Privacy header of incoming SIP messages. If the Privacy header has no remaining flags after the <strong>critical</strong> flag is removed, the system removes the Privacy header from the message.</td>
</tr>
<tr>
<td>Allow SSL 3.0 (change will cause system restart)</td>
<td>When selected, allows the system to support the SSL 3.0 protocol for HTTPS communication. Disabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.0 (change will cause system restart)</td>
<td>When selected, allows the system to support the TLS 1.0 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.1 (change will cause system restart)</td>
<td>When selected, allows the system to support the TLS 1.1 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Allow TLS 1.2 (change will cause system restart)</td>
<td>When selected, allows the system to support the TLS 1.2 protocol for HTTPS communication. Enabled by default. Changing this setting causes the system to restart.</td>
</tr>
<tr>
<td>Refuse TLS connections with DHE key size less than</td>
<td>This setting enables you to select a Diffie-Hellman key size of 1024 or 2048 bits. <strong>Caution:</strong> If you select 2048 bits, TLS connections from the RealPresence DMA system to your other video conferencing devices may not work if the other devices do not support this higher security setting.</td>
</tr>
</tbody>
</table>

3. Click **Update** to save the settings.

**Restrict Security Ciphers**

The RealPresence DMA system comes with default ciphers enabled for each security protocol that you allow.

The ciphers are applied to communication that occurs on the management network interface and/or the signaling network interface.

You can restrict the ciphers for the security protocols that you allow, but Polycom recommends that you use the default settings unless you’re knowledgeable about ciphers and the consequences of removing specific ciphers.
Warning: If you remove ciphers that your browser or a client is using, you may be locked out of the RealPresence DMA management interface and connections with other devices may be terminated.

Procedure

1. Go to Admin > Server > Security Settings.
2. Click Management Cipher Selection to choose the ciphers to be applied on the management interface based on the allowed security protocols, as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the cipher.</td>
</tr>
<tr>
<td>Class</td>
<td>The classes of security that include the cipher.</td>
</tr>
<tr>
<td>Security protocol and FIPS mode</td>
<td>Lists the security protocols and FIPS mode. Yes and No indicate whether the protocol or FIPS mode uses the individual ciphers.</td>
</tr>
<tr>
<td>Default</td>
<td>Indicates whether the cipher is enabled as a RealPresence DMA system default setting for the different security protocols and FIPS mode.</td>
</tr>
</tbody>
</table>

If you modify the ciphers that are selected, you can use the Yes and No indicators in this column to reconfigure the settings to the original defaults if necessary.

3. Click Signaling Cipher Selection to choose the ciphers to be applied on the signaling interface based on the allowed security protocols, as described in the preceding table.
4. Click Update to save the settings.

Encryption

The following table lists the product capabilities that are supported but not necessarily required.

Requirements vary based on the customer environment.

<table>
<thead>
<tr>
<th>Application</th>
<th>Security Function</th>
<th>Description</th>
<th>Encryption Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>System passwords</td>
<td>Confidentiality Integrity</td>
<td>/etc/shadow</td>
<td>N/A</td>
</tr>
<tr>
<td>DMA passwords</td>
<td>Confidentiality Integrity</td>
<td>Application passwords stored in database</td>
<td>N/A</td>
</tr>
<tr>
<td>SIPS</td>
<td>ConfidentialityIntegrity Authentication</td>
<td>SIP signaling (Diffie-Hellman key exchange)</td>
<td>TLS (NSS) SSLv3 TLS v1.0, v1.1, v1.2</td>
</tr>
<tr>
<td>Application</td>
<td>Security Function</td>
<td>Description</td>
<td>Encryption Protocol</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Confidentiality, Integrity, Authentication</td>
<td>Web admin traffic REST API (Diffie-Hellman key exchange)</td>
<td>TLS (NSS) SSLv3/TLS v1.0, v1.1, v1.2</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>Authentication, Confidentiality</td>
<td>H.323 signaling</td>
<td>H.235 Authentication</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Confidentiality, Integrity</td>
<td>Licensing</td>
<td>N/A</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Confidentiality, Integrity</td>
<td>Licensing, Digital signatures: License Key</td>
<td>N/A</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Signature</td>
<td>Licensing, Digital signatures: Cer8com's ECDSA</td>
<td>OpenSSL</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Signature</td>
<td>Licensing, Digital signatures: OpenSSL's core cryptography library</td>
<td>OpenSSL</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Confidentiality, Integrity</td>
<td>Trusted Storage: OpenSSL's core cryptography library</td>
<td>OpenSSL</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Confidentiality, Integrity</td>
<td>Node-to-node communication</td>
<td>Custom with AES-128</td>
</tr>
<tr>
<td>TURN signal</td>
<td>Authentication</td>
<td>Allows the setup of media channels for videoconferencing calls for products that are present outside the core network, for example, on the external side of firewall/NAT devices</td>
<td>UDP/TCP, which carries MD5 hashed authentication data and message integrity is protected by SHA1</td>
</tr>
<tr>
<td>Access proxy</td>
<td>Confidentiality</td>
<td>Provides videoconferencing products outside the firewall (external to the network) the ability to connect to HTTPS, LDAP, and XMPP servers located inside the core network over encrypted TLS channels</td>
<td>Same as SIP Signal (Active)</td>
</tr>
<tr>
<td>Application</td>
<td>Security Function</td>
<td>Description</td>
<td>Encryption Protocol</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>VC2 provisioning proxy</td>
<td>Confidentiality</td>
<td>Provides provisioning of parameters for SIP registrar/proxy and user access details to the videoconferencing products over encrypted TLS channels</td>
<td>Same as SIP Signal (Active)</td>
</tr>
<tr>
<td>SSH</td>
<td>Authentication</td>
<td>Provides a remote control/management interface over an encrypted SSH channel</td>
<td>SSH v2.0</td>
</tr>
<tr>
<td>Tunnel (encryption mode is disabled in Russia release)</td>
<td>Authentication</td>
<td>Provides a dedicated connection between (2) OpenVPN-enabled devices, such as (2) DMAs, residing on either side of the firewall to minimize impacts to firewall policies and still provide connectivity for videoconferencing products.</td>
<td>TLS v1.0 UDP or TCP</td>
</tr>
</tbody>
</table>
Security Certificates

Topics:

▪ How Certificates are Used
▪ Accepted Certificates
▪ Certificate Signing Requests
▪ Installing Certificates
▪ Removing Certificates

Certificates are used between devices within your video conferencing environment (such as servers and endpoints) to authenticate the devices and to support encryption.

Certificates confirm that the servers within your infrastructure can communicate and have the option to encrypt the data. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a public key infrastructure (PKI).

The certificate authority (CA) is a single centralized authority such as an enterprise’s IT department, or a commercial CA that each computer on the network is configured to trust. Each server on the network has a public certificate that identifies it. When a client connects to a server, the server shows its signed public certificate to the client. The CA signs the public certificates of those servers that clients should trust. Trust is established because the certificate has been signed by the CA, and the client has been configured to trust the CA.

Related Links
Set Up Security

How Certificates are Used

The RealPresence DMA system uses certificates in the following ways:

1. The RealPresence DMA system presents its certificate to the remote end. For example:
   ▪ When a user logs into the RealPresence DMA system’s browser-based management interface, the RealPresence DMA system offers a certificate to identify itself to the browser (client).
     
     The RealPresence DMA system’s certificate must have been signed by a certificate authority and the browser must be configured to trust that certificate authority.
     
     If trust cannot be established, most browsers allow connection anyway, but display a dialog to the user, requesting permission.

   ▪ When the RealPresence DMA system connects to a Microsoft Active Directory server, it may present a certificate to identify itself.

     If Active Directory is configured to require a client certificate (this is not the default), the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface. Active Directory must be configured to trust the certificate authority, or it rejects the certificate and the connection fails.

   ▪ When the RealPresence DMA system connects to a Microsoft Exchange server (if the calendaring service is enabled), it may present a certificate to the server to identify itself.
Unless the **Allow unencrypted calendar notifications from Exchange server** security option is enabled, the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface. The Microsoft Exchange server must be configured to trust the certificate authority. Otherwise, the Microsoft Exchange Server integration status remains **Subscription pending** indefinitely, the RealPresence DMA system doesn't receive calendar notifications, and incoming meeting request messages are only processed approximately every 4 minutes.

2. The RealPresence DMA system validates the certificate of a remote server. For example:
   - When the RealPresence DMA system connects to a Polycom MCU configured for secure communications, a certificate may be used to identify the MCU (server) to the RealPresence DMA system (client). This can be configured in the RealPresence DMA system.
   - When performing call signaling requiring TLS, the RealPresence DMA system presents its certificate to the connecting client (one-way TLS). If the **Require mutual authentication (validation of client certificates)** SIP Settings option is enabled, then both ends validate each other's certificates (mutual TLS).

3. The RealPresence DMA system validates the certificate of a client. For example:
   - For incoming SIP connections, the RealPresence DMA system may check the client's certificate. This can be configured in the RealPresence DMA system (see **Selecting a Security Mode**).

### Accepted Certificates

Certificates come in several forms (encoding and protocol).

The following table shows the forms that can be installed in the RealPresence DMA system.

<table>
<thead>
<tr>
<th>Encoding</th>
<th>Protocol / File Type</th>
<th>Description and Installation Method</th>
</tr>
</thead>
</table>
| PEM (Base64-encoded ASCII text) | PKCS #7 protocol P7B file | Certificate chain containing:
   - A signed certificate for the system, authenticating its public key
   - The CA’s public certificate
   - Sometimes intermediate certificates
   Upload file or paste into text box. |
<p>| CER (single certificate) file | Signed certificate for the system, authenticating its public key. Upload file or paste into text box. |
| Certificate text              | Encoded certificate text copied from CA’s email or secure web page. Paste into text box. |</p>
<table>
<thead>
<tr>
<th>Encoding</th>
<th>Protocol / File Type</th>
<th>Description and Installation Method</th>
</tr>
</thead>
</table>
| DER (binary format using ASN.1 Distinguished Encoding Rules) | PKCS #12 protocol PFX file | Certificate chain containing:  
- A signed certificate for the system, authenticating its public key  
- A private key for the system  
- The CA's public certificate  
- Sometimes intermediate certificates  
Upload file. |
| PKCS #7 protocol P7B file | Certificate chain containing:  
- A signed certificate for the system, authenticating its public key  
- The CA's public certificate  
- Sometimes intermediate certificates  
Upload file. |
| CER (single certificate) file | Signed certificate for the system, authenticating its public key.  
Upload file. |

**Certificate Signing Requests**

You can create a certificate signing request (CSR) to obtain a certificate signed by a trusted certificate authority that uniquely identifies the RealPresence DMA system within your public key infrastructure.

After you initially install the RealPresence DMA system, it uses a default, self-signed certificate.

When you create a CSR, the system populates the request with the information you provide, including subject alternative name (SAN) extensions. The default system-generated SAN extensions, which vary depending on your configuration, display in the CSR. You can change these values or add more extensions if needed.

Use fully qualified domain names (FQDN) for required SAN-DNS extensions. A certificate authority (CA) may reject a CSR if it contains only short host names. If you include the SAN extensions listed in the **Optional Fields** column, the resulting certificate will allow clients and other servers to access the system using any of the values (short host names, FQDNs, or IP addresses) without encountering certificate warnings or errors. Ensure that you use a CA that can accept all of the CSR fields and SAN extensions required for your configuration.

**Note:** The RealPresence DMA system supports a single identity certificate.
Certificate Signing Request Requirements for a Core Configuration

When you create a certificate signing request (CSR) for a RealPresence DMA system with a core configuration, the system populates the CSR with the information you provide, including subject alternative name (SAN) extensions.

The following table lists the required and optional fields for core-configured systems, including single-server, High Availability, and superclustered configurations.

Note: All IP addresses and FQDNs are private in a core configuration.

<table>
<thead>
<tr>
<th>Required and Optional CSR Fields for a Core Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
</tr>
<tr>
<td>• Single server</td>
</tr>
<tr>
<td>• Single server in a supercluster</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>• Two servers (High Availability active-passive)</td>
</tr>
<tr>
<td>• Two-servers in a supercluster (High Availability active-passive)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Configuration</td>
</tr>
<tr>
<td>------------------------------------</td>
</tr>
<tr>
<td>• Two servers (High Availability</td>
</tr>
<tr>
<td>active-active)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Certificate Signing Request Requirements for an Edge or Combination Configuration**

When you create a certificate signing request (CSR) for a RealPresence DMA system with an edge or combination configuration, the system populates the CSR with the information you provide, including subject alternative name (SAN) extensions.

**Attention:** If you add HTTPS proxy next hops with a host header filter, you must specify the host FQDNs as subject alternative names (SANs) in the Certificate Signing Request for the RealPresence DMA system.

The following table lists the required and optional fields for edge and combination-configured systems, including single-server and High Availability configurations.
## Required and Optional CSR Fields for an Edge or Combination Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Required Fields</th>
<th>Optional Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single server</strong></td>
<td>• <strong>Common Name</strong>: Public fully qualified domain name (FQDN)</td>
<td>• <strong>SAN-DNS</strong>: Host name</td>
</tr>
<tr>
<td></td>
<td>• <strong>SAN-DNS</strong>: Public FQDN</td>
<td>• <strong>SAN-DNS</strong>: Private FQDN</td>
</tr>
<tr>
<td></td>
<td>• <strong>SAN-DNS</strong>: Private FQDN of HTTPS application server (if an HTTPS proxy next hop is configured with a host header filter)</td>
<td>• <strong>SAN-DNS</strong>: Private IP address</td>
</tr>
<tr>
<td></td>
<td>• Country</td>
<td>• <strong>SAN-DNS</strong>: Public IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Public IP address</td>
</tr>
<tr>
<td><strong>Two servers (High Availability active-passive)</strong></td>
<td>• <strong>Common Name</strong>: Public FQDN</td>
<td>• <strong>SAN-IP</strong>: Private IP address</td>
</tr>
<tr>
<td></td>
<td>• <strong>SAN-DNS</strong>: Public FQDN</td>
<td>• <strong>SAN-IP</strong>: Private virtual IP address</td>
</tr>
<tr>
<td></td>
<td>• Country</td>
<td>• <strong>SAN-IP</strong>: Private physical server 1 IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Private physical server 2 IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Public virtual IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Private virtual IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Private physical server 1 IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Private physical server 2 IP address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>SAN-IP</strong>: Public virtual IP address</td>
</tr>
</tbody>
</table>
Create a Certificate Signing Request
You can create a certificate signing request (CSR) to obtain a certificate signed by a trusted certificate authority that uniquely identifies the RealPresence DMA system within your public key infrastructure.
This method uses the private key generated at the time of software installation.
Note: Obtaining certificates for Microsoft environments. If you're configuring the RealPresence DMA system to support Polycom's solution for the Microsoft Office Communication Server or Skype for Business environment, you can use Microsoft's Certificate Wizard to request and obtain a PFX file (a password-protected PKCS12 file containing a private key and public key for the system, and the CA's certificate). See Polycom's Microsoft Solution Deployment Guide, available at support.polycom.com, for information about using the Certificate Wizard.

Procedure

1. Go to Admin > Server > Certificates.
   By default, the system is configured to use a self-signed certificate.

2. To see details of the public certificate currently being used to identify the system to other computers:
   a. In the list, select the SSL certificate.
   b. Click Display Details.
      The Certificate Details window displays. If this is the default self-signed certificate, Organizational Unit is Self Signed Certificate.
   c. Click OK.

3. In the Actions list, select Create Certificate Signing Request.
   If you've created a signing request before, you're asked if you want to use your existing certificate request or generate a new one. Elect to generate a new one.

4. Enter the identifying information for your RealPresence DMA system as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name (CN)</td>
<td>Defaults to the FQDN of the system's management interface, as defined by the virtual host name and domain specified on the Network page. Editable.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>The cryptographic hash algorithm used to sign the CSR.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>Subdivision of organization. Specify up to three OUs. Optional.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Optional.</td>
</tr>
<tr>
<td>City or locality (L)</td>
<td>Optional.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>Optional.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Two-character country code.</td>
</tr>
<tr>
<td>Subject alternative name (SAN)</td>
<td>The area you can use to add, edit, or delete SAN extensions in this CSR.</td>
</tr>
<tr>
<td>Value</td>
<td>A list of SAN extensions and their values currently associated with the CSR.</td>
</tr>
</tbody>
</table>

5. Click Add to open the Add Subject Alternative Name (SAN) dialog.
6. Select an Extension type from the list and enter the associated Extension value.
7. Click OK.
8. Repeat steps 5-7 as needed to add SAN extensions required for your configuration.
9. To change an existing SAN extension, select it from the Value list and click Edit.
10. To delete a SAN value, select it from the Value list and click Delete.
11. Click OK to generate the CSR.
   The Certificate Signing Request dialog displays the encoded request.
12. Copy the entire contents of the Encoded Request box (including the text -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----) and submit it to your certificate authority.
   Depending on the CA, your CSR may be submitted via email or by pasting into a web page.
13. Click OK.
   When your CA has processed your request, it sends you a signed public certificate for your RealPresence DMA system. Some certificate authorities also send intermediate certificates and/or root certificates. Depending on the certificate authority, these certificates may arrive as email text, email attachments, or be available on a secure web page.
   The RealPresence DMA system accepts PKCS#7 or PKCS#12 certificate chains or single certificates.

Caution: Some CSR fields should not be modified. When you submit the CSR to your CA, make sure that the CA doesn't modify any of the predefined SAN fields or the X.509v3 Key Usage or Extended Key Usage fields. Changes to these fields may make your system unusable.

View an Encoded Certificate Signing Request
You can view an encoded certificate signing request and copy it for submission to your CA.

Procedure
1. Ensure the information in the Summary section is correct.
2. In the Encoded Request box, select and copy the encoded certificate request text, if desired.
3. Click OK.

Add a Subject Alternative Name (SAN) Extension
You can add a SAN extension when you create a certificate signing request (CSR).

Procedure
1. Go to Admin > Server > Certificates.
2. Click Create Certificate Signing Request.
3. Enter any required certificate information in the appropriate fields.
4. In the Subject Alternative Name (SAN) area, click Add.
5. Enter information in the following fields as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension type</td>
<td>Allows you to choose one of several types of SAN extensions to add to the CSR.</td>
</tr>
<tr>
<td>Extension value</td>
<td>The value of the SAN extension.</td>
</tr>
</tbody>
</table>
6. Click OK.

**Edit a Subject Alternative Name (SAN) Extension**

You can edit an existing SAN extension when you create a certificate signing request (CSR).

**Procedure**

1. Go to Admin > Server > Certificates.
2. Click Create Certificate Signing Request.
3. Enter any required certificate information in the appropriate fields.
4. In the Subject Alternative Name (SAN) area, click Edit.
5. Change information in the following fields as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension type</td>
<td>Allows you to choose one of several types of SAN extensions to add to the CSR.</td>
</tr>
<tr>
<td>Extension value</td>
<td>The value of the SAN extension.</td>
</tr>
</tbody>
</table>

**Installing Certificates**

You can add, edit, and remove certificates from the system.

**Note:** When you make changes in the RealPresence DMA system that cause a new certificate to be generated, or when you install a new certificate, you may need to refresh or reload the browser before you log back in to the management user interface. If you refresh the browser and still see outdated information or cannot download log files in the RealPresence DMA system, you should clear the browser's cache.

This section includes the following topics:

**View Installed Certificates**

You can view installed certificates on the Certificate Settings page.

**Procedure**

>` Go to Admin > Server > Certificates.

The list of installed certificates appears, as described by the following table:
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable OCSP         | Enables the use of Online Certificate Status Protocol as a means of obtaining the revocation status of a certificate presented to the system. If **OCSP responder URL** is not specified, the system checks the certificate's AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder:  
  ▪ If there is none, the certificate fails validation.  
  ▪ Otherwise, the system sends the OCSP request to the responder identified in the certificate.  
If **OCSP responder URL** is specified, the system sends the OCSP request to that responder. The responder returns a message indicating whether the certificate is good, revoked, or unknown.  
If **OCSP certificate** is specified, the response message must be signed by the specified certificate's private key. |
| OCSP responder URL  | Identifies the responder to be used for all OCSP requests, overriding the AIA field values. If **OCSP certificate** is specified, the response message must be signed by the specified certificate's private key. |
| OCSP certificate    | Select a certificate to require OCSP response messages to be signed by the specified certificate's private key.                                                                                               |
| Store OCSP          | Saves the OCSP configuration.                                                                                                                                                                               |
| Configuration       |                                                                                                                                                                                                            |
| Identifier          | Common name of the certificate.                                                                                                                                                                              |
| Purpose             | Kind of certificate:  
  ▪ Server SSL is the RealPresence DMA system's public certificate, which it presents to identify itself. By default, this is a self-signed certificate, not trusted by other devices.  
  ▪ Trusted Root CA is the root certificate of a certificate authority that the RealPresence DMA system trusts.  
  ▪ Intermediate CA is a CA certificate that trusted root CAs issue themselves to sign certificate signing requests (reducing the likelihood of their root certificate being compromised). If the RealPresence DMA system trusts the root CA, then the chain consisting of it, its intermediate CA certificates, and the server certificate will all be trusted. |
| Expiration          | Expiration date of certificate.                                                                                                                                                                             |

**Display Certificate Details**

You can select a certificate from the list of installed certificates and view its information.

**Procedure**

1. Go to **Admin > Server > Certificates**.
2. Select a certificate from the list and click **Display Details**.
3. View the certificate details, as outlined in the following table:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Info</td>
<td>Purpose and alias of the certificate.</td>
</tr>
<tr>
<td>Issued To</td>
<td>Information about the entity to which the certificate was issued and the certificate serial number.</td>
</tr>
<tr>
<td>Issued By</td>
<td>Information about the issuer.</td>
</tr>
<tr>
<td>Validity</td>
<td>Issue and expiration dates.</td>
</tr>
<tr>
<td>Misc Info</td>
<td>The signature algorithm used in the certificate.</td>
</tr>
<tr>
<td>Fingersprints</td>
<td>SHA1 and MD5 fingerprints (checksums) for confirming certificate.</td>
</tr>
<tr>
<td>Subject Alternative Names</td>
<td>Additional identities bound to the subject of the certificate.</td>
</tr>
<tr>
<td></td>
<td>For the RealPresence DMA system, this should include the virtual and physical FQDNs, short host names, and IP addresses of the system.</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>Indicates the purposes for which the certificate can be used.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system's certificate is used for both server and client connections, so this should always contain at least serverAuth and clientAuth.</td>
</tr>
</tbody>
</table>

4. When finished viewing the certificate details, click **OK**.

**Install a Certificate Authority's Certificate**

This procedure is not necessary if you obtain a certificate chain that includes a signed certificate for the RealPresence DMA system, your certificate authority's public certificate, and any intermediate certificates.

Use this procedure to add a trusted certificate authority, either an in-house or commercial CA.

**Caution:** **Installing or removing certificates requires a restart**

Installing or removing certificates requires a system restart and terminates all active conferences. When you install or remove a certificate, the change is made to the certificate store immediately, but the system cannot implement the change until it restarts and reads the changed certificate store. You do not need to restart and apply a change immediately. You can perform multiple installs or removals before restarting and applying the changes. When you are finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update.

**Procedure**

1. Go to **Admin > Server > Certificates**.

   The installed certificates are listed. The **Trusted Root CA** entries, if any, represent the certificate authorities whose public certificates are already installed on the RealPresence DMA system and are thus trusted.

2. If you're using a certificate authority that isn't listed, obtain a copy of your certificate authority's public certificate.
The certificate must be either a single X.509 certificate or a PKCS#7 certificate chain. If it's ASCII text, it's in PEM format, and starts with the text ---BEGIN CERTIFICATE-----. If it's a file, it can be either PEM or DER encoded.

3. In the Actions list, select Add Certificates.
4. In the Add Certificates dialog, do one of the following:
   - If you have a file, click Upload certificate, enter the password (if any) for the file, and browse to the file or enter the path and file name.
   - If you have PEM-format text, copy the certificate text, click Paste certificate, and paste it into the text box below.

5. Click OK.
6. Verify that the certificate appears in the list as a Trusted Root CA.
7. Click Restart to Apply Saved Changes.
8. Click OK to restart the system so that the certificate changes can take effect.

Install a Signed Certificate

Before installing a certificate or certificate chain provided by the certificate authority, be sure that you received the certificate or certificate chain in one of the following forms:

- A PFX, P7B, or single certificate file that you have saved on your computer.
- PEM-format encoded text that you received in an e-mail or on a secure web page.

Installing or removing certificates requires a system restart and terminates all active conferences. When you install or remove a certificate, the change is made to the certificate store immediately, but the system cannot implement the change until it restarts and reads the changed certificate store.

You do not need to restart and apply a change immediately. You can perform multiple installs or removals before restarting and applying the changes. When you are finished making changes, you must select Restart to Apply Saved Changes to restart the system and finish your update. Ensure there are no active conferences before you restart the system.

Procedure
1. When you receive your certificate(s), return to Admin > Server > Certificates.
2. In the Actions list, select Add Certificates.
3. In the Add Certificates dialog, do one of the following:
   - If you have a PFX, P7B, or single certificate file, click Upload certificate, enter the password (if any) for the file, and browse to the file or enter the path and file name.
   - If you have PEM-format text, copy the certificate text, click Paste certificate, and paste it into the text box below. You can paste multiple PEM certificates one after the other.
4. Click OK.
5. To verify that the new signed certificate has replaced the default self-signed certificate:
   a. In the list of certificates, once again select the Server SSL certificate.
   b. In the Actions list, select Display Details.
      The Certificate Details dialog appears.
   c. Review the information under Issued To and Issued By to confirm that the self-signed default certificate has been replaced by your signed public certificate from the certificate authority.
   d. Click OK.
6. Click **Restart to Apply Saved Changes**.
7. Click **OK** to restart the system so that the certificate changes can take effect.

**Removing Certificates**

Installing or removing certificates requires a system restart and terminates all active conferences.

When you install or remove a certificate, the change is made to the certificate store immediately, but the system cannot implement the change until it restarts and reads the changed certificate store.

You are not required to restart and apply a change immediately. You can perform multiple installs or removals before restarting and applying the changes. When you are finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Ensure there are no active conferences before you restart the system.

There are two kinds of certificate removal:

- Removing the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.
- Removing the signed certificate currently in use so that the system reverts to using the default self-signed certificate. Removing a signed certificate *will not remove* the certificate of the Trusted Root CA that signed it, or any intermediate certificates provided by that certificate authority.

**Remove a Trusted Root CA's Certificate**

You can remove the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.

**Procedure**

1. Go to **Admin > Server > Certificates**.
2. In the certificates list, select the certificate you want to delete.
3. Under **Actions**, select **Display Details** and confirm that you have selected the correct certificate.
4. Click **OK**.
5. Under **Actions**, select **Delete Certificate**.
6. Click **Yes** to confirm.
7. Click **OK**.
8. Click **Restart to Apply Saved Changes**.
9. Click **OK** to restart the system so that the certificate changes can take effect.

**Remove a Signed Certificate**

If you remove a signed certificate, the system reverts to the default self-signed certificate.

Removing a signed certificate *will not remove* the certificate of the Trusted Root CA that signed it, or any intermediate certificates provided by that certificate authority.

**Procedure**

1. Go to **Certificates**.
2. In the **Actions** list, select **Revert to Default Certificate**.
3. When asked to confirm, click **Yes**.

   A message informs you that the system has reverted to a self-signed certificate.
4. Click **OK**.

5. Click **Restart to Apply Saved Changes**.

6. Click **OK** to restart the system so that certificate changes can take effect.

7. After the system restarts, log back in, return to **Admin > Server > Certificates**, and verify that the system has reverted to the default self-signed certificate:
   
   a. In the list of certificates, select the **Server SSL** certificate.
   
   b. Under **Actions**, select **Display Details**.
      
      The **Certificate Details** dialog appears.
   
   c. Review the information under **Issued To** and **Issued By** to confirm that the default self-signed certificate has replaced the CA-signed certificate.
   
   d. Click **OK**.
History Retention Settings

Topics:

- Configure History Record Retention

The RealPresence DMA system is pre-configured with the number of history records of various types to retain.

When the retention limit has been reached for a record type, the system purges a specific number of the oldest records of that type.

The following table shows the retention limit for each record type, and how many are purged at a time when the retention limit is reached. The values specified are for each cluster, not the total for the entire supercluster.

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Retention Limit</th>
<th>Number of Records Purged when Limit is Reached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration history</td>
<td>505,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Registration signaling</td>
<td>2,000,000</td>
<td>20,000</td>
</tr>
<tr>
<td>Call history</td>
<td>505,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Call signaling history</td>
<td>12,625,000</td>
<td>125,000</td>
</tr>
<tr>
<td>Conference history</td>
<td>202,000</td>
<td>2,000</td>
</tr>
<tr>
<td>CDR export history</td>
<td>11,000</td>
<td>1,000</td>
</tr>
</tbody>
</table>

The history retention settings are supercluster-wide (the clusters are not independently configured).

Configure History Record Retention

You can specify whether to retain registration history records, and if so, whether to include registration keep-alive messages.

You can also specify how many repeated low-value signaling records to retain.

Only users with the Auditor role can configure history retention settings.

Procedure

1. Log into the system as a user with the Auditor role.
2. Go to Admin > History Retention Settings.
3. Specify whether to record registration history, and if so, whether to include keep-alive messages.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable recording of registration history</td>
<td>Enables the system to retain call server registration records.</td>
</tr>
</tbody>
</table>
| Include keep-alive messages in registration history | If selected, the call server history includes the keep-alive messages sent by registered endpoints and the call server's responses.  
Selecting this option significantly increases the number of call server registration records per period of time. |
| Number of repeated low-value signaling event records to retain | The number of less-important signaling messages (such as INFO messages about in-call status) to retain for a given call (from 0 to 10; default is 3).  
Once the limit is reached, subsequent messages of that type are processed, but not recorded in the call signaling history. |

4. Specify how many low-value signaling records to retain.
5. Click **Update**.
6. Click **OK**.
Superclustering

Topics:

- About Superclustering
- Verify DNS FQDN Resolution
- View Details for RealPresence DMA Systems
- Create or Join a Supercluster
- Organize Territories and Assign Responsibilities
- Busy Out a Cluster
- Stop Using a Cluster
- Start Using a Cluster
- Remove a Cluster from a Supercluster

The following topics describe the RealPresence DMA system's superclustering capability.

Related Links
Rejoin the Cluster to the Supercluster

About Superclustering

Two RealPresence DMA systems can be configured as a co-located two-server cluster to enhance the reliability of the systems by providing redundancy.

To provide even greater reliability, geographic redundancy, and improved network traffic management, multiple RealPresence DMA systems (either single-server or two-server systems) in distributed locations can be combined into a supercluster.

A supercluster is a set of up to 10 RealPresence DMA clusters that are geographically dispersed, but still centrally managed. The clusters in a supercluster are all peers. There's no master or primary cluster. All have local copies of the same data store, which is kept consistent via replication.

The common data store enables all of the superclustered RealPresence DMA systems to share data, including users, groups, conference rooms, services, site topology, dial plans, bandwidth management, endpoint registrations, usage reporting, status monitoring, conference manager configuration, call server configuration, and integrations. Sharing and replicating data also enables any cluster in the supercluster to configure or reconfigure the shared data.

Up to three clusters in a supercluster can function as conference managers, hosting conference rooms and managing pools of MCUs.

To use superclustering, you must have at least one DNS server. The host names (virtual and physical) of every cluster in the supercluster must be resolvable by all the other clusters. Each physical host name, physical IP address, and virtual host name must have A/AAAA records on your DNS server(s).

In addition to a DNS server, you must have at least one network time protocol (NTP) server.
Verify DNS FQDN Resolution

Before creating a supercluster, you should verify that the DNS can resolve all FQDNs of all clusters that will become part of the supercluster.

Procedure

1. Go to Admin > Troubleshooting Utilities > Ping.
2. Ping the FQDNs (virtual and physical) of each cluster that will be part of the supercluster.

View Details for RealPresence DMA Systems

The DMAs list includes information about RealPresence DMA clusters.

If the system you’re logged in to isn’t (and hasn’t been) part of a supercluster, the list contains only that system.

Procedure

1. Go to Integrations > DMAs.
2. View the following details about the RealPresence DMA systems on your network.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates whether the cluster is superclustered and whether it’s in service. Some clusters may be part of a supercluster but not currently be in service.</td>
</tr>
<tr>
<td>Host name</td>
<td>Virtual host name of the cluster's management interface.</td>
</tr>
<tr>
<td>Model</td>
<td>Type of system. Currently, only RealPresence DMA systems may join a supercluster.</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the system.</td>
</tr>
<tr>
<td>IP address</td>
<td>Virtual IP address of the cluster's management interface.</td>
</tr>
</tbody>
</table>

Create or Join a Supercluster

You can create or join a supercluster on the DMAs page.

To create a new supercluster, you must log in to a standalone cluster and invite a different standalone cluster to join the supercluster. Be sure to log in to the cluster that has the data and configuration you want to preserve as that data becomes the shared supercluster data store. After the cluster you invite accepts the invitation, both systems become clusters in the new supercluster. The system you invited to join has its local data store largely replaced by a copy of the data store from the system you’re logged in to.

For example, if a cluster is integrated with your RealPresence Resource Manager system, log in to that cluster and invite other clusters to join the cluster you’re logged in to. The site topology and user-to-device association data from the RealPresence Resource Manager system will be replicated throughout the supercluster.
Note: When you invite a system to join a supercluster, active calls will continue uninterrupted on the system from which you send an invitation to join. However, all active calls will be terminated on the system you invite to join the supercluster.

Procedure

1. Go to Integrations > DMAs.
2. Under ACTIONS, click Invite to Join Supercluster.
3. Complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or IP address</td>
<td>The host name or IP address of the system you invite to join the supercluster. We strongly recommend specifying the FQDN of the virtual management interface for the cluster invited to join. You may specify an IP address; however, the virtual and physical host names of every cluster in the supercluster must be resolvable by all the other clusters. In a split network configuration, the host names are associated with the management network interface.</td>
</tr>
<tr>
<td>User name</td>
<td>An administrator login name for the cluster you invite to join.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the administrator login.</td>
</tr>
</tbody>
</table>

4. Click OK.

A prompt warns you that the invited system will restart and its local data will be overwritten.

5. Click Yes to confirm.

The cluster you’re logged in to connects to the cluster you invited to join and establishes the supercluster. The invited cluster obtains supercluster-wide configuration and data (this can take some time depending on the size of the data set). The system informs you when the process is complete and the invited cluster is ready to restart.

6. Click OK.

You may need to restart the browser or clear the browser cache in order to log back into the system.

7. Log in to the system that joined the supercluster and verify that the Supercluster Status pane of the dashboard shows the correct number of clusters.

8. Go to Integrations > DMAs, and verify that the status of each RealPresence DMA cluster is In service.

9. Reassign territory responsibilities as needed.

Organize Territories and Assign Responsibilities

In a supercluster, the responsibility for most of the RealPresence DMA system's functionality, including Active Directory and Exchange integration, device registration, call handling, and conference room (VMR) hosting, is assigned among the clusters using site topology territories.

You can assign a set of responsibilities to each territory, and you can assign a primary cluster and a backup cluster for each territory. When the primary cluster is online, it controls the territory and carries out all of the responsibilities belonging to the territory. When the primary cluster is offline, the backup cluster assumes control of the territory and carries out all of the territory's responsibilities.
A maximum of three territories can host conference rooms.

A standalone (not superclustered) RealPresence DMA system has a single default territory for which it’s the primary cluster, without backup. When this cluster joins a supercluster, it still has the same single default territory, is still the primary cluster for the default territory, and still has no backup cluster. Essentially, one cluster is responsible for everything, and the others do nothing. Therefore, immediately after forming a new supercluster, you need to organize and create territories and assign functional responsibilities to those territories.

**Procedure**

1. Create your site topology data if you have not already done so, or integrate with a RealPresence Resource Manager system to obtain the data.

2. Organize your sites into territories that best distribute responsibilities and workload among the clusters of your supercluster.

   For example, with a five-cluster supercluster, do one of the following:
   - Create four territories, assign a primary cluster for each, and assign the fifth cluster as backup for all four.
   - Create five territories, assign a primary cluster for each, and make each cluster the backup for one of the other territories.
   - Use some hybrid of the preceding options that best suits your enterprise network’s distribution of sites, users, and traffic.

3. Create the territories, assign their functional responsibilities, and assign primary and backup clusters.

   If you’ve integrated with a RealPresence Resource Manager system, site topology data comes from that system and cannot be edited in the RealPresence DMA system. You must create the territories you need in the RealPresence Resource Manager system.

**Related Links**

Site Topology on page 414

---

**Busy Out a Cluster**

When you **Busy Out** a selected cluster, you slowly decrease the use of the selected cluster:

- Existing calls and conferences on the selected cluster continue, but no new conferences are allowed to start. New calls are allowed to start only if they’re associated with existing conferences. Registrations are rejected, except for endpoints currently involved in calls. The cluster ceases to manage bandwidth.

- Territories for which the selected cluster has primary responsibility and a different cluster has backup responsibility are transferred to the backup cluster.

- Registrations are seamlessly transferred to the backup cluster (for endpoints that support this). Bandwidth usage data for ongoing calls is seamlessly transferred to the backup cluster.

**Procedure**

1. Go to Integrations > DMAs.
2. Select the cluster to busy out and click **Busy Out**.
3. Click **OK** to confirm the action.
Stop Using a Cluster

When you Stop Using a selected cluster, you take the cluster immediately out of service.

This creates the following results:

- Existing calls and conferences on the selected cluster are disconnected. No new calls or conferences are allowed to start. All registrations are rejected. The cluster ceases to manage bandwidth.
- Territories for which the selected cluster has primary responsibility and a different cluster has backup responsibility are transferred to the backup cluster.
- Registrations are seamlessly transferred to the backup cluster (for endpoints that support this). Bandwidth usage data for ongoing calls is seamlessly transferred to the backup cluster.

Procedure
1. Go to Integrations > DMAs.
2. Select the cluster to stop using and click Stop Using.
3. Click OK to confirm the action.

Start Using a Cluster

When you Start Using a cluster, you put the selected cluster back into service:

- New calls and conferences are allowed to start. The cluster begins bandwidth management.
- The cluster assumes control of any territories for which it has primary responsibility, or for which it has backup responsibility and the primary cluster is offline.
- For territories for which the restarted cluster is the primary, existing calls and conferences on the backup cluster continue, but no new conferences are allowed to start. New calls are allowed to start only if they’re associated with existing conferences. The backup cluster ceases to manage bandwidth.
- Registrations are seamlessly transferred to the restarted primary cluster, where supported by the endpoint. Bandwidth usage data for ongoing calls is seamlessly transferred to the restarted primary cluster.

Procedure
1. Go to Integrations > DMAs.
2. Select the cluster to start using and click Start Using.
3. Click OK to confirm the action.

Remove a Cluster from a Supercluster

You can remove a cluster from the supercluster, which reinitializes it as a new stand-alone cluster.

It retains the data and configuration from the supercluster (including site topology), but that data is no longer synchronized to the common data store. If the cluster you plan to remove is responsible for any territories (as primary or backup), you must first reassign those territories.

Note: There’s no mechanism for shutting down an entire supercluster. If you want to shut down all clusters in a supercluster, you must shut down and restart one cluster at a time.
Procedure

1. Go to Integrations > DMAs.
2. Select the cluster to remove and click Remove From Supercluster.
3. Click OK to confirm the action.
External Device Configuration

Topics:

- External SIP Peers
- External H.323 Gatekeepers
- External H.323 Session Border Controllers
- External Skype for Business Systems

This section provides an introduction to configuring external devices for use with the Polycom RealPresence DMA system.

It includes:
External SIP Peers

Topics:

- Multiple External SIP Peers
- SIP Peer Availability and Third-Party Network Devices
- View External SIP Peers
- Add an External SIP Peer
- Edit an External SIP Peer
- SIP Peer Postliminary Output Format Options
- Free Form Template Variables
- To Header and Request-URI Header Examples
- Add an Authentication Credential Entry
- Edit an Authentication Credential Entry
- Add an External Registration
- Edit an External Registration

In a RealPresence DMA system, you can add or remove SIP servers or devices from a list of SIP peers to which the system can route calls and from which it may receive calls.

Defining external SIP peers is a supercluster-wide configuration. A RealPresence DMA supercluster can provide proxy service for any or all domains in the enterprise. This allows the SIP function to be distributed, but managed centrally and may reduce the need for external SIP peer servers, other than SIP session border controllers (SBCs). SIP SBCs to be reached by prefix-based dialing need to be added as external SIP peers.

Note: SBCs to be reached by a dial rule using the Resolve to external address or Resolve to IP address action are configured on a per-site basis. For most configuration, SBCs should be configured on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC for the originating site.

Related Links
Add an External SIP Peer on page 133
Edit a Site on page 428
View External SIP Peers on page 132
Edit an External SIP Peer on page 139

Multiple External SIP Peers

The RealPresence DMA system can use multiple SIP peers to resolve dial strings.

If a SIP peer experiences an outage, it is marked as unresponsive, and the RealPresence DMA system stops using it until it becomes responsive again. If you add multiple SIP peers to the system, you can
configure how the system selects which SIP peer to use to resolve dial strings by using a dial rule with the Resolve to external SIP peer action.

When you configure a dial rule that uses the Resolve to external SIP peer action, you can choose which of two selection policies the system uses to resolve dial strings to SIP peers. If you select All in parallel (forking), the system tries all SIP peers simultaneously. If you select Weighted round-robin, you can assign each SIP peer a weight, with a higher weight giving a SIP peer higher priority, and the system tries each SIP peer sequentially according to the SIP peer's assigned weight. You can change the weight for each SIP peer as necessary. Unresponsive SIP peers are considered only when there are no responsive peers that can complete the call.

**SIP Peer Availability and Third-Party Network Devices**

The RealPresence DMA system periodically uses SIP OPTIONS messages to verify connectivity with SIP peers.

If a SIP peer fails to respond or responds with a specified set of status codes, the system removes that SIP peer from service. In some situations, a third-party device can respond on behalf of the SIP peer. If the RealPresence DMA system receives any other status code when the queried SIP peer is experiencing an outage, that SIP peer could incorrectly be marked as healthy.

Because of this, it is possible for a SIP peer's service status to enter a flapping state. In this scenario, the RealPresence DMA system attempts to use the incorrectly marked SIP peer, but when the SIP peer fails to respond, the RealPresence DMA system removes the SIP peer from service. However, the RealPresence DMA system receives a non-specified status code response for the next availability query, so puts the SIP peer back in service.

**View External SIP Peers**

The RealPresence DMA system displays a list of External SIP Peers and some of the configuration details for each peer.

You can view the list for reference.

**Procedure**

» Go to Integrations > External SIP Peers.

The following table describes the fields in the list of External SIP Peers.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the external SIP peer.</td>
</tr>
<tr>
<td>Type</td>
<td>If a + icon displays, hover over the icon to see the type of the external SIP peer. An external SIP peer can be one of the following types: • DMA Licensed - the external SIP peer will count calls. • DMA Subordinate - the external SIP peer will not count calls. • Other - the external SIP peer will not count calls. • Microsoft - the external SIP peer will not count calls.</td>
</tr>
</tbody>
</table>
**UDP TCP TLS**
Provides a visual responsiveness status of each SIP peer for the UDP, TCP, and TLS protocols, depending on what **Transport type** the system is configured to use when contacting this SIP peer. If the **Transport type** is set to **Auto Detect**, the system may use multiple transport types and may display an icon indicating responsiveness for each type it uses. Responsiveness status for each SIP peer in the list is updated every 10 seconds by default.

---

**Description**
Brief description of the external SIP peer.

**Next hop address**
Fully qualified domain name (FQDN) or IP address of the external SIP peer.

**Prefix range**
The dial string prefix(es) assigned to this external SIP peer. If your dial plan uses the **Dial services by prefix** dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.

**Enabled**
Indicates whether the system is using the external SIP peer.

**External registrations**
Indicates whether the system is registered with the external SIP peer so that it can route calls to it. Displays **Active** if there are any **External Registrations** defined for this SIP peer that are enabled.

---

**Related Links**
- [External SIP Peers](#) on page 131
- [Device Authentication](#) on page 408
- [SIP Peer Postliminary Output Format Options](#) on page 147

---

**Add an External SIP Peer**
You can add one or more external SIP peers to your RealPresence DMA system. When you add a new external SIP peer, it is enabled by default.

**Procedure**
1. Go to **Integrations > External SIP Peers**.
2. Click the **Add** button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Peer name or number. Must be unique among SIP peers.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of the external SIP peer.</td>
</tr>
</tbody>
</table>
### Type

An external SIP peer can be one of the following types:

- **DMA Licensed** - the external SIP peer will count calls.
- **DMA Subordinate** - the external SIP peer will not count calls.
- **Other** - the external SIP peer will not count calls.
- **Microsoft** - the external SIP peer will not count calls. For a Microsoft Office Communications Server, Lync Server or Skype for Business Server, select Microsoft. Selecting **Microsoft** implicitly adds the **Destination network** value to the Domain List (if not already there) and automatically selects the Postliminary settings that are correct for most deployments in Microsoft environments, but you can modify them if necessary.

**Note:** Selecting **Microsoft** enables the **Skype Integration** tab.

### Next hop address

Fully qualified domain name (FQDN), host name, or IP address of the SIP peer. Spaces after the name are not allowed.

If you specify a domain/host name, the system routes calls to this peer by using DNS to resolve the address. The DNS server that the system uses must contain the required records (NAPTR, SRV, and/or A/AAAA).

**Note:** If you’re configuring a Lync 2013 or Skype for Business SIP Peer, the **Next hop address** should be the FQDN or IP address of the Lync or Skype front-end pool, not an individual Lync, or Skype server within a pool.

### Destination network

Host name, FQDN, or network domain label of the SIP peer, with or without port and URL parameters.

If specified, this value by default replaces the non-user portion of a URL (after the @ symbol) of the To header and Request-URI for forwarded messages, and the Request-URI for REGISTER messages.

If **Type** is set to Microsoft, this field is required and is used for the peer’s domain.

**Note:** This field is used as the SIP domain for Polycom RealConnect conferences.

### Port

The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, enter it here.

**Note:** For a Lync or Skype for Business SIP peer, the port should be 5061.

If left blank, the system determines the port via DNS.

### Transport type

The transport protocol to use when contacting this SIP peer. The default is **TCP**.

**Auto detect** tells the system to select the protocol using DNS as specified in RFC 3263, and is not valid if **Next hop address** is a numeric IP address instead of a host/domain name.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use route header    | Add a route header with the peer’s **Next hop address** value to the message.  
Applies to both forwarded messages and external REGISTER messages.  
If not selected, the only valid Request-URI configurations are those that use the peer’s **Next hop address** value for the URI host.  
**Note:** Disable this option for Lync or Skype for Business SIP peers that will accept content sessions from Polycom RealPresence ContentConnect applications through the RealPresence DMA system. |
| Downgrade           | If selected, and if this peer doesn’t support TLS, the system can change the Request-URI schema from sips to sip and route the call to this peer.  
If not selected, the system routes a TLS call to this peer only if this peer supports TLS.                                                                                                                                                                                                                                                                                   |
| Prefix range        | The dial string prefix(es) assigned to this SIP peer.  
Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46).  
If your dial plan uses the **Dial services by prefix** dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.  
If your dial plan instead uses a rule that you create to apply the **Resolve to external SIP peer** action, there is no need to specify a prefix.  
Otherwise, the system applies the **SIP Routing** settings of the originating site for calls to endpoints outside the enterprise network.  
**Note:** For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer’s prefix is 123, the dial string for a call to alice@polycom.com must be one of the following:  
sip:123alice@polycom.com  
sips:123alice@polycom.com  
123alice                                                                                                                                                                                                 |
| Strip prefix        | If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.                                                                                                                                                                                                                                                                                                                                 |
| Register externally | Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as **pilot registration**).  
Select this option to enable the **External Registration** tab and configure the system to register with this external SIP peer, following the rules specified in RFC 3261.                                                                                                                                                                                                                     |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports SIP OPTIONS ping</td>
<td>If selected, the system sends SIP OPTIONS ping messages to the SIP peer to determine its responsiveness. See the Service Config &gt; Call Server Settings page for configuration options related to SIP OPTIONS ping messages.</td>
</tr>
</tbody>
</table>
| Domain list | If your dial plan uses a rule to apply the Resolve to external SIP peer action, you can restrict calls to this SIP peer to specific domains by adding the authorized domains to this list.  
If this list is empty, all domains can resolve to this peer.  
**Note:** In some circumstances (depending on network topology and configuration), dialing loops can develop if you don’t restrict SIP peers to specific domains. |
| Add new domain | Enter a domain and click **Add** to add it to the list of authorized domains. |
| Authorized domains | List of administrative domains, contained in the dial string, for which calls are routed to this SIP peer.  
Leave this list empty to route any call that matches the rule to this SIP peer.  
Select a domain and click **Remove** to remove it from the list. |

### Postliminary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enabled | If checked, the fields on this page are available and in effect. If unchecked, the fields are disabled and the original SIP signaling is passed unchanged to the SIP peer.  
This field is unchecked by default if you select a **Type** of Microsoft when adding a SIP peer.  
**Note:** Polycom recommends leaving postliminary scripts disabled for Microsoft SIP peers to ensure proper signaling operation with calls to external Lync or Skype for Business systems. |
| Use output format | Enables dial string transformations using the **To header options** and Request-URI options below instead of a customized script.  
**Note:** The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select **Use customized script**.  
To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes. |
<p>| To header options | Specify the format of the <strong>To</strong> header in messages sent to this peer. |
| Copy all parameters of original <strong>To</strong> headers | Copies any parameters included in the original <strong>To</strong> header to the <strong>To</strong> header sent to this peer. This setting applies to all format options. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Select a predefined format from the list, or select <strong>Free Form Template</strong> and define the format in the associated <strong>Template</strong> field.</td>
</tr>
<tr>
<td>Template</td>
<td></td>
</tr>
<tr>
<td>Request URI options</td>
<td>Specify the format of the Request-URI.</td>
</tr>
<tr>
<td>Format</td>
<td>Select a predefined format from the list, or select <strong>Free Form Template</strong> and define the format in the associated <strong>Template</strong> field.</td>
</tr>
<tr>
<td>Template</td>
<td></td>
</tr>
<tr>
<td>Use customized script</td>
<td>Enables you to write or paste an executable script in JavaScript in the text box below. Using such a script enables you to more flexibly define dial string and message format transformations to be applied.</td>
</tr>
<tr>
<td></td>
<td>Type (or paste) the postliminary script you want to apply. Then click <strong>Debug this Script</strong> to test the script with different variables.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you change settings in the <strong>Use output format</strong> section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script. The functions in the generated script return string values and accept string parameters.</td>
</tr>
<tr>
<td>Authentication</td>
<td>On this tab, you can configure SIP digest authentication for this SIP peer and add or edit authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>SIP authentication must be enabled and configured in <strong>Device Authentication</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the <strong>Resolve to external SIP peer</strong> action. If another dial rule action, such as <strong>Resolve to external address</strong>, is applied to the call, there is no association to this peer and its authentication settings are not used.</td>
</tr>
<tr>
<td>Outbound authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Handle authentication</strong> - When it receives a 401 (Unauthorized) response from this SIP peer, the call server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pass authentication</strong> - When it receives a 401 response from this SIP peer, the call server passes it to the source of the request.</td>
</tr>
<tr>
<td>Outbound proxy authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Handle proxy authentication</strong> - When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the call server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pass proxy authentication</strong> - When it receives a 407 response from this SIP peer, the call server passes it to the source of the request.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inbound authentication</td>
<td>Determines if the RealPresence DMA system requires authentication credentials when an outbound call receives an inbound request.</td>
</tr>
<tr>
<td></td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always challenge peer</strong> - inbound requests will be challenged for authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Never challenge peer</strong> - inbound requests will not be challenged for authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>When you enable SIP authentication for endpoints, it is not currently possible to define behavior regarding unauthenticated ports.</td>
</tr>
<tr>
<td></td>
<td>When you enable SIP authentication for both standard and custom ports and define an external SIP peer using the custom port, the system routes calls to the custom port. However, the Contact header in the outbound SIP INVITE message from the RealPresence DMA system contains port 5060. This causes the in-dialogue message to be rejected with a 401 response.</td>
</tr>
<tr>
<td></td>
<td>(table of authentication entries)</td>
</tr>
<tr>
<td></td>
<td>Lists the authentication credential entries defined for use with this SIP peer, showing the realm in which the entry is valid and the user name. Click <strong>Add</strong> to add authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>When choosing authentication credentials to present to this SIP peer, the call server looks first at the entries listed here. If there is none with the correct realm, it looks for an appropriate entry on the <strong>Device Authentication</strong> page.</td>
</tr>
<tr>
<td></td>
<td>Skype integration</td>
</tr>
<tr>
<td></td>
<td>This tab contains fields necessary to integrate with a Lync 2013 or Skype for Business server, and is enabled when you select a <strong>Type</strong> of <strong>Microsoft</strong> on the <strong>External SIP Peers</strong> tab.</td>
</tr>
<tr>
<td>Maximum Polycom conference</td>
<td>The maximum number of Polycom conference contacts that the RealPresence DMA system attempts to publish to this SIP peer.</td>
</tr>
<tr>
<td>contacts to publish</td>
<td>If this value is lower than the number of conference contacts configured for presence publishing, the system displays an alert.</td>
</tr>
<tr>
<td></td>
<td>The maximum Polycom conference contacts to publish is 25,000.</td>
</tr>
<tr>
<td>Enable RealConnect</td>
<td>Indicates that this Lync or Skype for Business SIP peer should be cascaded with Polycom MCUs for on-premises Polycom RealConnect conferences. If enabled, this SIP peer is used to resolve Lync or Skype conference IDs.</td>
</tr>
<tr>
<td>conferences</td>
<td>This option must be enabled for this SIP peer to appear in the <strong>Available SIP peers</strong> area in dial rules that use the <strong>Resolve to Skype conference ID</strong> action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option does not apply to RealConnect conferences with external Lync or Skype for Business systems.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Skype account URI | The account ID the RealPresence DMA system should use when resolving Lync or Skype for Business conference IDs. Any user account on the Lync or Skype server can be used. This field is enabled when **Enable RealConnect conferences** is checked.

MCU pool order | The MCU pool order this Lync or Skype for Business SIP peer uses for Polycom MCUs that provide Skype AVMCU cascade functionality. If you leave this option unchecked, the **Dial to on-premises RealConnect conference** dial rule will use the **MCU pool order** you selected for the rule in **Admin > Call Server > Dial Rules**. This field is enabled when **Enable RealConnect conferences** is checked.

CsTrustedApplication ServiceGruu | The GRUU value that the system should use when communicating with Lync or Skype for Business clients that connect to VMR conferences. When enabled, the RealPresence DMA system includes the text field value in the signaling it sends to Lync or Skype for Business clients that have joined VMR conferences. This identifies the RealPresence DMA system as a trusted application when communicating with these clients. Enabling this option can prevent calls from Lync or Skype for Business clients to VMRs that are many hours in length from disconnecting unexpectedly. See the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide* for information on obtaining the GRUU value to populate this field.

External registrations | Lists any outbound registration configurations associated with this SIP peer and lets you add, edit, or delete registrations. Multiple registrations may be associated with a SIP peer.

Enable external registrations | Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as pilot registration). Select this option to enable external registrations and configure the system to register with this external SIP peer.

#### 4. Click **OK**.

**Related Links**

- [External SIP Peers](#) on page 131
- [Device Authentication](#) on page 408
- [SIP Peer Postliminary Output Format Options](#) on page 147

## Edit an External SIP Peer

You can edit an existing external SIP peer when necessary.
Procedure

1. Go to **Integrations > External SIP Peers**.
2. Select the SIP peer to revise and click **Edit**.
3. Revise the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Peer name or number. Must be unique among SIP peers.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description of the external SIP peer.</td>
</tr>
<tr>
<td>Type</td>
<td>An external SIP peer can be one of the following types:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>DMA Licensed</strong> - The external SIP peer will count calls.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>DMA Subordinate</strong> - The external SIP peer will not count calls.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Other</strong> - The external SIP peer will not count calls.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Microsoft</strong> - the external SIP peer will not count calls. For a Microsoft Office Communications Server, Lync Server or Skype for Business Server, select <strong>Microsoft</strong>. Selecting <strong>Microsoft</strong> implicitly adds the <strong>Destination network</strong> value to the <strong>Domain List</strong> (if not already there) and automatically selects the <strong>Postliminary</strong> settings that are correct for most deployments in Microsoft environments, but you can modify them if necessary. <strong>Note</strong>: Selecting <strong>Microsoft</strong> enables the <strong>Skype Integration</strong> tab.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Fully qualified domain name (FQDN), host name, or IP address of the SIP peer. Spaces after the name are not allowed.</td>
</tr>
<tr>
<td></td>
<td>If you specify a domain/host name, the system routes calls to this peer by using DNS to resolve the address. The DNS server that the system uses must contain the required records (NAPTR, SRV, and/or A/AAAA). <strong>Note</strong>: If you are configuring a Lync 2013 or Skype for Business SIP Peer, the <strong>Next hop address</strong> should be the FQDN or IP address of the Lync or Skype front-end pool, not an individual Lync or Skype server within a pool.</td>
</tr>
<tr>
<td>Destination network</td>
<td>Host name, FQDN, or network domain label of the SIP peer, with or without port and URL parameters.</td>
</tr>
<tr>
<td></td>
<td>If specified, this value by default replaces the non-user portion of a URL (after the @ symbol) of the To header and Request-URI for forwarded messages, and the Request-URI for REGISTER messages. <strong>Note</strong>: If <strong>Type</strong> is set to Microsoft, this field is required and is used for the peer’s domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This field is used as the SIP domain for Polycom RealConnect conferences.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, enter it here.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a Lync or Skype for Business SIP peer, the port should be 5061.</td>
</tr>
<tr>
<td></td>
<td>If left blank, the system determines the port via DNS.</td>
</tr>
<tr>
<td>Transport type</td>
<td>The transport protocol to use when contacting this SIP peer. The default is <strong>TCP</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Auto detect</strong> tells the system to select the protocol using DNS as specified in RFC 3263, and is not valid if <strong>Next hop address</strong> is a numeric IP address instead of a host/domain name.</td>
</tr>
<tr>
<td>Use route header</td>
<td>Add a route header with the peer's <strong>Next hop address</strong> value to the message.</td>
</tr>
<tr>
<td></td>
<td>Applies to both forwarded messages and external REGISTER messages.</td>
</tr>
<tr>
<td></td>
<td>If not selected, the only valid Request-URI configurations are those that use the peer's <strong>Next hop address</strong> value for the URI host.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Disable this option for Lync or Skype for Business SIP peers that will accept content sessions from Polycom RealPresence ContentConnect applications through the RealPresence DMA system.</td>
</tr>
<tr>
<td>Downgrade</td>
<td>If selected, and if this peer doesn't support TLS, the system can change the <strong>Request-URI</strong> schema from sips to sip and route the call to this peer.</td>
</tr>
<tr>
<td></td>
<td>If not selected, the system routes a TLS call to this peer only if this peer supports TLS.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix(es) assigned to this SIP peer. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46). If your dial plan uses the <strong>Dial services by prefix</strong> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution. If your dial plan instead uses a rule that you create to apply the <strong>Resolve to external SIP peer</strong> action, there is no need to specify a prefix. Otherwise, the system applies the <strong>SIP Routing</strong> settings of the originating site for calls to endpoints outside the enterprise network. <strong>Note:</strong> For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to <a href="mailto:alice@polycom.com">alice@polycom.com</a> must be one of the following: sip:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a> sips:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a> 123alice</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.</td>
</tr>
<tr>
<td>Register externally</td>
<td>Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as <strong>pilot registration</strong>). Select this option to enable the <strong>External Registration</strong> tab and configure the system to register with this external SIP peer, following the rules specified in RFC 3261.</td>
</tr>
<tr>
<td>Supports SIP OPTIONS ping</td>
<td>If selected, the system sends SIP OPTIONS ping messages to the SIP peer to determine its responsiveness. See the <strong>Service Config &gt; Call Server Settings</strong> page for configuration options related to SIP OPTIONS ping messages.</td>
</tr>
<tr>
<td>Domain List</td>
<td>If your dial plan uses a rule to apply the <strong>Resolve to external SIP peer</strong> action, you can restrict calls to this SIP peer to specific domains by adding the authorized domains to this list. If this list is empty, all domains can resolve to this peer. <strong>Note:</strong> In some circumstances (depending on network topology and configuration), dialing loops can develop if you don’t restrict SIP peers to specific domains.</td>
</tr>
<tr>
<td>Add new domain</td>
<td>Enter a domain and click <strong>Add</strong> to add it to the list of authorized domains.</td>
</tr>
</tbody>
</table>
### Authorized domains

List of administrative domains, contained in the dial string, for which calls are routed to this SIP peer.

Leave this list empty to route any call that matches the rule to this SIP peer.

Select a domain and click **Remove** to remove it from the list.

### Postliminary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>If checked, the fields on this page are available and in effect. If unchecked, the fields are disabled and the original SIP signaling is passed unchanged to the SIP peer.</td>
</tr>
<tr>
<td></td>
<td>This field is unchecked by default if you select a <strong>Type</strong> of <strong>Microsoft</strong> when adding a SIP peer.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Polycom recommends leaving postliminary scripts disabled for Microsoft SIP peers to ensure proper signaling operation with calls to external Lync or Skype for Business systems.</td>
</tr>
<tr>
<td>Use output format</td>
<td>Enables dial string transformations using the <strong>To header options</strong> and <strong>Request-URI options</strong> below instead of a customized script.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select <strong>Use customized script</strong>.</td>
</tr>
<tr>
<td></td>
<td>To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes.</td>
</tr>
<tr>
<td>To header options</td>
<td>Specify the format of the <strong>To</strong> header in messages sent to this peer.</td>
</tr>
<tr>
<td>Copy all parameters of original <strong>To</strong> headers</td>
<td>Copies any parameters included in the original <strong>To</strong> header to the <strong>To</strong> header sent to this peer. This setting applies to all format options.</td>
</tr>
<tr>
<td>Format <strong>Template</strong></td>
<td>Select a predefined format from the list, or select <strong>Free Form Template</strong> and define the format in the associated <strong>Template</strong> field.</td>
</tr>
<tr>
<td>Request URI options</td>
<td>Specify the format of the Request-URI.</td>
</tr>
<tr>
<td>Format <strong>Template</strong></td>
<td>Select a predefined format from the list, or select <strong>Free Form Template</strong> and define the format in the associated <strong>Template</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use customized script</td>
<td>Enables you to write or paste an executable script in Javascript in the text box below. Using such a script enables you to more flexibly define dial string and message format transformations to be applied. Type (or paste) the postliminary script you want to apply. Then click <strong>Debug this Script</strong> to test the script with different variables. <strong>Note:</strong> When you change settings in the <strong>Use output format</strong> section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script. The functions in the generated script return string values and accept string parameters.</td>
</tr>
<tr>
<td>Authentication</td>
<td>On this tab, you can configure SIP digest authentication for this SIP peer and add or edit authentication credentials. SIP authentication must be enabled and configured in <strong>Device Authentication</strong>. <strong>Note:</strong> The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the <strong>Resolve to external SIP peer</strong> action. If another dial rule action, such as <strong>Resolve to external address</strong>, is applied to the call, there is no association to this peer and its authentication settings are not used.</td>
</tr>
<tr>
<td>Outbound authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Handle authentication</strong> - When it receives a 401 (Unauthorized) response from this SIP peer, the call server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pass authentication</strong> - When it receives a 401 response from this SIP peer, the call server passes it to the source of the request.</td>
</tr>
<tr>
<td>Outbound proxy authentication</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Handle proxy authentication</strong> - When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the call server presents its authentication credentials. If there are no authentication credentials for the specified realm, the response is passed back to the originating call leg.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pass proxy authentication</strong> - When it receives a 407 response from this SIP peer, the call server passes it to the source of the request.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inbound authentication</td>
<td>Determines if the RealPresence DMA system requires authentication credentials when an outbound call receives an inbound request.</td>
</tr>
<tr>
<td></td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always challenge peer</strong> - inbound requests will be challenged for authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Never challenge peer</strong> - inbound requests will not be challenged for authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>When you enable SIP authentication for endpoints, it is not currently possible to define behavior regarding unauthenticated ports.</td>
</tr>
<tr>
<td></td>
<td>When you enable SIP authentication for both standard and custom ports and define an external SIP peer using the custom port, the system routes calls to the custom port. However, the Contact header in the outbound SIP INVITE message from the RealPresence DMA system contains port 5060. This causes the in-dialogue message to be rejected with a 401 response.</td>
</tr>
<tr>
<td>(table of authentication entries)</td>
<td>Lists the authentication credential entries defined for use with this SIP peer, showing the realm in which the entry is valid and the user name. Click <strong>Add</strong> to add authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>When choosing authentication credentials to present to this SIP peer, the call server looks first at the entries listed here. If there is none with the correct realm, it looks for an appropriate entry on the <strong>Device Authentication</strong> page.</td>
</tr>
<tr>
<td>Skype Integration</td>
<td>This tab contains fields necessary to integrate with a Lync 2013 or Skype for Business server, and is enabled when you select a <strong>Type of Microsoft</strong> on the <strong>External SIP Peers</strong> tab.</td>
</tr>
<tr>
<td>Maximum Polycom conference contacts to publish</td>
<td>The maximum number of Polycom conference contacts that the RealPresence DMA system attempts to publish to this SIP peer.</td>
</tr>
<tr>
<td></td>
<td>If this value is lower than the number of conference contacts configured for presence publishing, the system displays an alert.</td>
</tr>
<tr>
<td></td>
<td>The maximum Polycom conference contacts to publish is 25,000.</td>
</tr>
<tr>
<td>Enable RealConnect conferences</td>
<td>Indicates that this Lync or Skype for Business SIP peer should be cascaded with Polycom MCUs for on-premises Polycom RealConnect conferences. If enabled, this SIP peer is used to resolve Lync or Skype conference IDs.</td>
</tr>
<tr>
<td></td>
<td>This option must be enabled for this SIP peer to appear in the <strong>Available SIP peers</strong> area in dial rules that use the <strong>Resolve to Skype conference ID</strong> action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option does not apply to RealConnect conferences with external Lync or Skype for Business systems.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Skype account URI</td>
<td>The account ID the RealPresence DMA system should use when resolving Lync or Skype for Business conference IDs. Any user account on the Lync or Skype server can be used.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled when <strong>Enable RealConnect conferences</strong> is checked.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order this Lync or Skype for Business SIP peer uses for Polycom MCUs that provide Skype AVMCU cascade functionality. If you leave this option unchecked, the <strong>Dial to on-premises RealConnect conference</strong> dial rule will use the <strong>MCU pool order</strong> you selected for the rule in <strong>Admin &gt; Call Server &gt; Dial Rules</strong>.</td>
</tr>
<tr>
<td></td>
<td>This field is enabled when <strong>Enable RealConnect conferences</strong> is checked.</td>
</tr>
<tr>
<td>CsTrustedApplication ServiceGruu</td>
<td>The GRUU value that the system should use when communicating with Lync or Skype for Business clients that connect to VMR conferences.</td>
</tr>
<tr>
<td></td>
<td>When enabled, the RealPresence DMA system includes the text field value in the signaling it sends to Lync or Skype for Business clients that have joined VMR conferences. This identifies the RealPresence DMA system as a trusted application when communicating with these clients.</td>
</tr>
<tr>
<td></td>
<td>Enabling this option can prevent calls from Lync or Skype for Business clients to VMRs that are many hours in length from disconnecting unexpectedly. See the <em>Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide</em> for information on obtaining the GRUU value to populate this field.</td>
</tr>
<tr>
<td>External registrations</td>
<td>Lists any outbound registration configurations associated with this SIP peer and lets you add, edit, or delete registrations. Multiple registrations may be associated with a SIP peer.</td>
</tr>
<tr>
<td>Enable external registrations</td>
<td>Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as <strong>pilot registration</strong>).</td>
</tr>
<tr>
<td></td>
<td>Select this option to enable external registrations and configure the system to register with this external SIP peer.</td>
</tr>
</tbody>
</table>

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

**Related Links**

- [Device Authentication](#) on page 408
- [External SIP Peers](#) on page 131
- [SIP Peer Postliminary Output Format Options](#) on page 147
SIP Peer Postliminary Output Format Options

The postliminary settings include several output format options for an external SIP peer:

**Related Links**
- Add an External SIP Peer on page 133
- Edit an External SIP Peer on page 139
- View External SIP Peers on page 132

**To Header Format Options**

The settings available on the **Format** list for the **To** header are described below.

If a user is present in the URI, the user is always preserved except when **Free Form Template** is selected.

**Use original request's To** - The To header from the original request is copied and used as is. Equivalent to template:

```
"#otdisplay#" <#otscheme#:#otuser#@#othost#>
```

**No Display, use original request's To** - The To header from the original request is copied and used. If a display parameter is present, it's removed. Equivalent to template:

```
<#otscheme#:#otuser#@#othost#
```

**With Display, use peer's next hop address as host** - URI's host is replaced with the **Next hop address** value for this peer. No other changes are made. Equivalent to template:

```
"#otdisplay#" <#pscheme#:#otuser#@#phost#>
```

**No Display, use original request's URL host** - The To header from the original request is copied, the URI is replaced with the host/IP portion of the original request's Request-URI. If a display parameter is present, it's removed. Equivalent to template:

```
<#pscheme#:#otuser#@#orhost#>
```

**No Display, use peer's Destination Network or next hop address** - Uses the **Destination network** value if specified, otherwise the peer's **Next hop address** value. If a display parameter is present, it's removed. Equivalent to template:

```
<#pscheme#:#otuser#@#pnetORphost#>
```

**Default To header for Microsoft** - Equivalent to template:

```
"#otdisplay#" <sip:#otuser#@#pnetORphost#>
```

**Free Form Template** - Format defined in associated **Template** field is used without further modification.
**Request-URI Header Format Options**

The settings available on the Format list for the Request-URI header are described below (RR= requires route header):

**Use original request's URI (RR)** - The original request's URI is copied and moved. Equivalent to template:

```
#orscheme#:#oruser#@#orhost#
```

**No user, original request's host (RR)** - The user in the original, if any, is removed, but the original host is used. Equivalent to template:

```
#orscheme#:#orhost#
```

**No user, configured peer's next hop address as host** - The user in the original, if any, is removed, and the host is replaced with the Next hop address value for this peer. Equivalent to template:

```
#pscheme#:#phost#
```

**Original user, configured peer's next hop address as host** - The user in the original is copied, but the host is replaced with the Next hop address value for this peer. Equivalent to template:

```
#pscheme#:#oruser#@#phost#
```

**Note:** If the peer's transport type is configured as TLS, this setting makes the Request-URI scheme sips even if the original Request-URI's scheme was sip. Some SIP peers, such as the Cisco SBC, won't accept sips in the Request-URI if other headers contain sip. If this problem exists, change Format to Free Form Template and in the Template field, change #pscheme# to #orscheme#.

**Use user as host (RR)** - Uses the user in the original, if specified, as the host value, otherwise the host value is used as is. Equivalent to template:

```
#orscheme#:#oruser# (but if no original user is present, the host value is used as is).
```

**No user, configured peer's Destination Network or next hop address** - Uses the Destination network value if specified, otherwise the peer's Next hop address value. Equivalent to template:

```
#pscheme#:#pnetORphost#
```

**Original user, configured peer's Destination Network or next hop address** - Uses the user in the original, if specified, but replaces the host with the Destination network value, if specified, or the peer's Next hop address value. Equivalent to template:

```
#pscheme#:#otuser#@#pnetORphost#
```
Default Request-URI for Microsoft - Equivalent to template:

```
sip:#oruser#@#pnetORphost#:#pport#;transport=#ptransport#
```

Request-URI for Microsoft without CSS - Equivalent to template:

```
sip:#phost#:#pport#;transport=#ptransport#
```

Free Form Template - Format defined in associated Template field is used without further modification.

**Free Form Template Variables**

In the Template fields on the Postliminary tab, and when specifying a Request-URI or other headers for outbound registration, you can use the variables in the following table entered as `#variable name#` (case insensitive).

The system replaces the variables with the corresponding values as shown below.

You can also use these variables (without `#` delimiters) in a customized script.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>otdisplay</td>
<td>Original To header's display name.</td>
</tr>
<tr>
<td>otuser</td>
<td>User portion of the original request's To header URL field.</td>
</tr>
<tr>
<td>othost</td>
<td>Host/IP portion of the original request's To header URL field.</td>
</tr>
<tr>
<td>otscheme</td>
<td>Original To header's URL scheme (sip, sips, tel).</td>
</tr>
<tr>
<td>phost</td>
<td>Peer's configured IP/FQDN (next hop address).</td>
</tr>
<tr>
<td>pscheme</td>
<td>Peer's configured scheme based on transport (sip, sips).</td>
</tr>
<tr>
<td>oruser</td>
<td>User portion of the original request's Request-URL field.</td>
</tr>
<tr>
<td>orhost</td>
<td>Host/IP portion of the original request's Request-URL field.</td>
</tr>
<tr>
<td>orscheme</td>
<td>Original request's URL scheme.</td>
</tr>
<tr>
<td>pnetORphost</td>
<td>Destination network parameter if specified, otherwise the peer's configured IP/FQDN.</td>
</tr>
<tr>
<td>pport</td>
<td>The port specified for this SIP peer.</td>
</tr>
<tr>
<td>ptransport</td>
<td>The transport type specified for this SIP peer.</td>
</tr>
</tbody>
</table>

In addition to the variables, you can enter any values acceptable for the Request-URI or To header.

For the Request-URI, the contents of the Template field specify only the URI portion of the full Request line. Depending on network configuration, a Route header may be required.
For the To header, the contents of the Template field specify the complete header except for the header name (To).

The @ symbol is always removed if no user is present in the result.

Related Links
Add an External Registration on page 152
Edit an External Registration on page 154

To Header and Request-URI Header Examples

The following tables show some examples of To header and Request-URI header transformations using free form template variables.

<table>
<thead>
<tr>
<th>Original To Header</th>
<th>Template</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:atest</td>
<td>sip:atest</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:otuser@#othost#</td>
<td>sip:user@host</td>
</tr>
<tr>
<td>sip:host</td>
<td>#otscheme#:otuser#@foo.bar</td>
<td>sip:foo.bar</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:otuser#@foo.bar</td>
<td>sip:<a href="mailto:user@foo.bar">user@foo.bar</a></td>
</tr>
<tr>
<td>sip:host</td>
<td>sips:#otuser#@foo.bar</td>
<td>sips:foo.bar</td>
</tr>
<tr>
<td>sip:user@host</td>
<td>#otscheme#:otuser#@#othost#</td>
<td>sip:user@toHeaderUrlHost</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Original Request-URI Header</th>
<th>Template</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayname <a href="">sip:user@host</a></td>
<td>#ordisplay# <a href="">sip:#oruser#@#orhost#</a></td>
<td>displayname <a href="">sip:user@host</a></td>
</tr>
</tbody>
</table>
Add an Authentication Credential Entry

You can add an authentication credential entry either for a specific external SIP peer or to the general list of outbound authentication credentials that the system uses if challenged by an external device.

Procedure

1. Go to Integrations > External SIP Peers.
2. In the Actions list, click Add.
3. In Add External SIP Peer, select Authentication.
4. Click Add to add an authentication entry.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Unique string that identifies the protection domain to which this set of credentials applies. Generally includes the host or domain name of the SIP peer. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for authentications in this realm.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for authentications in this realm.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

6. Click OK.

Related Links

Device Authentication on page 408
Edit an Authentication Credential Entry

You can edit an authentication credential entry either for a specific external SIP peer or from the general list of outbound credentials for the system.

Procedure
1. Go to Integrations > External SIP Peers.
2. Select the SIP peer of interest and click Edit.
3. In the Edit External SIP Peer dialog, select Authentication.
4. Select the authentication credential entry to revise and click Edit.
5. Edit the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Unique string that identifies the protection domain to which this set of credentials applies. Generally includes the host or domain name of the SIP peer. See RFC 2617 and RFC 3261.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for authentications in this realm.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for authentications in this realm.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>The password to use for authentications in this realm.</td>
</tr>
</tbody>
</table>

6. Click OK.

Related Links
Device Authentication on page 408

Add an External Registration

Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also known as pilot registration).

You can add external registration configurations that the RealPresence DMA system can use to register with the SIP peer that you are adding or editing.

Procedure
1. Go to Integrations > External SIP Peers.
2. In the Actions list, click Add.
3. In Add External SIP Peer, select External Registrations.
4. Click Add to add an external registration.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using this registration without deleting the registration information.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Address of record</td>
<td>The address of record with which the RealPresence DMA system registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@dma.polycom.com">1000@dma.polycom.com</a></td>
</tr>
<tr>
<td>Territory to perform registration</td>
<td>Responsibility for registering must be assigned to a territory, thus making the primary or backup RealPresence DMA cluster for the territory responsible, depending on which is active.</td>
</tr>
<tr>
<td>Contact address format</td>
<td>Select IP Address or DNS Name to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it resends the registration using its IP address or DNS name. Select Free Form to specify that the contact header should use the FQDN you enter. The external SIP peer must be able to resolve this FQDN.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for the authentication credentials if the external peer challenges the registration request.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for the authentication credentials if the external peer challenges the registration request.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Request-URI</td>
<td>The Request-URI to include when registering with this SIP peer, specified using the Free Form Template Variables (#delimited).</td>
</tr>
<tr>
<td>Other headers</td>
<td>Additional headers to include when registering with this SIP peer. Click Add to add a header. In the Add Header dialog, specify the header name and value(s), using the Free Form Template Variables (#delimited). Click Edit or Delete to edit or delete the selected header.</td>
</tr>
</tbody>
</table>

6. Click OK.

Related Links
Free Form Template Variables on page 149
Edit an External Registration

You can edit external registration configurations that the RealPresence DMA system can use to register with the SIP peer that you are editing.

Procedure

1. Go to Integrations > External SIP Peers.
2. Select the External Sip Peer to edit and in the Actions list, click Edit.
3. In Edit External SIP Peer, select External Registrations.
4. Select the external registration to revise and click Edit.
5. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using this registration without deleting the registration information.</td>
</tr>
<tr>
<td>Address of record</td>
<td>The address of record with which the RealPresence DMA system registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@dma.polycom.com">1000@dma.polycom.com</a></td>
</tr>
<tr>
<td>Territory to perform registration</td>
<td>Responsibility for registering must be assigned to a territory, thus making the primary or backup RealPresence DMA cluster for the territory responsible, depending on which is active.</td>
</tr>
<tr>
<td>Contact address format</td>
<td>Select IP Address or DNS Name to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it re-sends the registration using its IP address or DNS name. Select Free Form to specify that the contact header should use the FQDN you enter. The external SIP peer must be able to resolve this FQDN.</td>
</tr>
<tr>
<td>User name</td>
<td>The user name to use for the authentication credentials if the external peer challenges the registration request. <strong>Note:</strong> The authentication credentials specified here are specific to this SIP peer and are not tied to any other authentication configuration values.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for the authentication credentials if the external peer challenges the registration request.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Request-URI</td>
<td>The Request-URI to include when registering with this SIP peer, specified using the Free Form Template Variables (#delimited). <strong>Note:</strong> Request-URI and other headers are available only when Use route header is enabled in the External SIP Peers section.</td>
</tr>
</tbody>
</table>

6. Click OK.
Related Links
Free Form Template Variables on page 149
## External H.323 Gatekeepers

**Topics:**
- View External Gatekeepers
- Add an External Gatekeeper
- Edit an External Gatekeeper
- Add an External Gatekeeper with both an IPv4 and IPv6 Address

When an enterprise has multiple neighbored gatekeepers, each gatekeeper manages its own H.323 zone. When a call originates in one gatekeeper zone and that zone’s gatekeeper is unable to resolve the dialed address, it forwards the call to the neighbor gatekeeper(s) for resolution.

Defining external H.323 gatekeepers is a supercluster-wide configuration. A RealPresence DMA supercluster can manage multiple locations as a single H.323 zone, with the clusters acting as a single virtual gatekeeper. This allows the gatekeeper function to be geographically distributed, but managed centrally. A supercluster may eliminate the need for multiple zones and neighbor gatekeepers.

**Related Links**
- Add an External Gatekeeper on page 157
- Edit an External Gatekeeper on page 159
- Add a Dial Rule to a Dial Plan on page 309
- Add an External Gatekeeper with both an IPv4 and IPv6 Address on page 161

### View External Gatekeepers

You can view a list of any external gatekeepers that you have integrated with your RealPresence DMA system.

**Procedure**

» Go to Integrations > External H.323 Gatekeepers.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the neighbored gatekeeper.</td>
</tr>
</tbody>
</table>
| Type       | If a + icon displays, hover over the icon to see the type of the external gatekeeper. An external gatekeeper can be one of the following types:  
  • DMA Licensed - The external gatekeeper will count calls.  
  • DMA Subordinate - The external gatekeeper will not count calls.  
  • Other - The external gatekeeper will not count calls. |
| Description| Brief description of the gatekeeper.             |
Add an External Gatekeeper

You can add an external gatekeeper to your RealPresence DMA system. This is a supercluster-wide configuration.

**Procedure**

1. Go to Integrations > External H.323 Gatekeepers.
2. Click the Add button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Host name or IP address of the gatekeeper.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix(es) assigned to this neighbor gatekeeper. If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the system is using the neighbor gatekeeper.</td>
</tr>
</tbody>
</table>

---

### External Gatekeepers

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Gatekeeper name.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the external gatekeeper.</td>
</tr>
</tbody>
</table>
| Type            | If a + icon displays, hover over the icon to see the type of the external gatekeeper. An external gatekeeper can be one of the following types:  
• DMA Licensed - The external gatekeeper will count calls.  
• DMA Subordinate - The external gatekeeper will not count calls.  
• Other - The external gatekeeper will not count calls. |
<p>| Address         | Host name or IP address of the gatekeeper.                                  |
| RAS port        | The Registration, Admission and Status (RAS) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number. |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range for which the external gatekeeper is responsible. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49). If your dial plan uses the Dial services by prefix dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution. If your dial plan instead uses a rule that you create to apply the Resolve to external gatekeeper action, there is no need to specify a prefix.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this gatekeeper.</td>
</tr>
<tr>
<td>Prefer routed</td>
<td>If selected (the default), the system forces all calls to this gatekeeper to routed mode. This setting must be enabled to avoid interoperability issues with the RealPresence Resource Manager system and Avaya gatekeepers, and possibly others as well.</td>
</tr>
<tr>
<td>Authentication mode</td>
<td>In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to the external gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When selected, the system sends its H.235 credentials to the external gatekeeper. Clearing this check box stops the system from sending H.235 credentials to the external gatekeeper but does not delete the credentials.</td>
</tr>
<tr>
<td>Name</td>
<td>The H.235 name of the RealPresence DMA system.</td>
</tr>
<tr>
<td>Password</td>
<td>The H.235 password for the RealPresence DMA system.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Algorithm</td>
<td>The encryption algorithm selected for H.235 authentication.</td>
</tr>
<tr>
<td>Send test LRQ</td>
<td>Click to test the configuration by sending an LRQ message to the external gatekeeper.</td>
</tr>
<tr>
<td>Postliminary</td>
<td>A postliminary is an executable script, written in the JavaScript language, that defines dial string transformations to be applied before querying the external gatekeeper.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When selected, the postliminary script is enabled. When the check box is cleared, the postliminary script is turned off without deleting it.</td>
</tr>
</tbody>
</table>
### Edit an External Gatekeeper

You can edit the configuration of an existing external gatekeeper as needed.

**Procedure**

1. Go to Integrations > External H.323 Gatekeepers.
2. Select the gatekeeper to edit and click the **Edit** button.
3. Revise the fields described in the following table as needed:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Gatekeeper name.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the external gatekeeper.</td>
</tr>
</tbody>
</table>
| Type     | If a + icon displays, hover over the icon to see the type of the external gatekeeper. An external gatekeeper can be one of the following types:  
  - **DMA Licensed** - The external gatekeeper will count calls.  
  - **DMA Subordinate** - The external gatekeeper will not count calls.  
  - **Other** - The external gatekeeper will not count calls. |
| Address  | Host name or IP address of the gatekeeper.                                 |
| RAS port | The Registration, Admission and Status (RAS) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number. |

---

Related Links

- Device Authentication on page 408
- External H.323 Gatekeepers on page 156
### Column

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prefix range</strong></td>
</tr>
<tr>
<td><strong>Strip prefix</strong></td>
</tr>
<tr>
<td><strong>Prefer routed</strong></td>
</tr>
<tr>
<td><strong>Authentication mode</strong></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
</tr>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Confirm password</strong></td>
</tr>
<tr>
<td><strong>Send test LRQ</strong></td>
</tr>
<tr>
<td><strong>Postliminary</strong></td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
</tr>
</tbody>
</table>
Add an External Gatekeeper with both an IPv4 and IPv6 Address

When adding a neighbor gatekeeper, you can specify only one IP address.

In an IPv4 plus IPv6 environment, you can use two separate dial rules to enable calls to resolve to a neighbor gatekeeper’s IPv4 or IPv6 address.

Requests from endpoints with IPv4 addresses will be forwarded to the gatekeeper’s IPv4 address, and requests from endpoints with IPv6 addresses will be forwarded to the gatekeeper’s IPv6 address.

Procedure

1. Add the neighbor gatekeeper using its IPv4 address.
2. Add the neighbor gatekeeper a second time using its IPv6 address.
3. Add one Resolve to external gatekeeper dial rule that specifies the neighbor gatekeeper’s IPv4 address entry (and no other gatekeepers).
4. Add another Resolve to external gatekeeper dial rule that specifies the neighbor gatekeeper’s IPv6 address entry (and no other gatekeepers).

Related Links

External H.323 Gatekeepers on page 156
### External H.323 Session Border Controllers

#### Topics:
- View External H.323 SBCs
- Add an External H.323 SBC
- Edit an External H.323 SBC

In an H.323 environment, H.323 session border controllers (SBCs) regulate access across the firewall. You can add or remove H.323 SBCs that the system can use to reach endpoints outside the enterprise network by prefix-based dialing. When you add, edit, or delete H.323 SBCs, the configurations are supercluster-wide.

H.323 SBCs that are added to the **External H.323 SBC** page are reached by prefix-based dialing.

SBCs to be reached by a dial rule using the **Resolve to IP address** action (rule 6 of the default dial plan) are configured on a per-site basis.

In general, H.323 SBCs should be configured on a per-site basis, so that calls to endpoints outside the enterprise network are routed to the SBC assigned to the originating site.

There are three reasons to configure an H.323 SBC on the **External H.323 SBC** page:
- To create a prefix service that allows dialing through the specific SBC by prefix. An SBC configured on this page must have a prefix or prefix range assigned to it and can only be reached by dialing its prefix(es).
- To define a postliminary script to be applied when dialing through the specific SBC.
- For bandwidth management.

The RealPresence DMA system is capable of performing call admission control (CAC) while processing an LRQ from a neighbor gatekeeper. This allows the system to reject the call for resource or policy reasons early in the setup process (in response to the LRQ), rather than waiting until later in the call setup.

In order to perform early CAC, the RealPresence DMA system must know the caller's media address, which is not provided in the LRQ and is unknowable for an ordinary gatekeeper. If the gatekeeper is also an SBC, however, it proxies the media. The RealPresence DMA system can assume that its media address is the same as its signaling address, and proceed with early CAC. The RealPresence DMA system performs early CAC only in response to LRQs received from SBCs configured on the **External H.323 SBC** page.

### View External H.323 SBCs

You can view a list of external H.323 session border controllers (SBCs) that you have added to your RealPresence DMA system.

#### Procedure
- Go to **Integrations** > **External H.323 SBCs**.

The following table describes the fields in the list:
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the SBC.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the SBC.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the SBC.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix(es) assigned to this SBC.</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the Dial services by prefix dial rule (in the</td>
</tr>
<tr>
<td></td>
<td>default dial plan) to route calls to services, all dial strings beginning</td>
</tr>
<tr>
<td></td>
<td>with an assigned prefix are forwarded to this SBC for resolution.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether the system is using the SBC.</td>
</tr>
</tbody>
</table>

**Add an External H.323 SBC**

You can add an external H.323 session border controller (SBC) to your RealPresence DMA system.

**Procedure**

1. Go to Integration > External H.323 SBCs.
2. In the Actions list, click Add.

The following table describes the fields in the Add External H.323 SBC dialog.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Clearing this check box lets you stop using an external SBC without</td>
</tr>
<tr>
<td></td>
<td>deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>SBC unit name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the External H.323 SBC list.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the SBC.</td>
</tr>
<tr>
<td>Port</td>
<td>The SBC's port number. Leave set to 1720 unless you know the unit is</td>
</tr>
<tr>
<td></td>
<td>using a non-standard port number.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range assigned to this SBC. Required.</td>
</tr>
<tr>
<td></td>
<td>Enter a single prefix (44), a range of prefixes (44-47), or multiple</td>
</tr>
<tr>
<td></td>
<td>prefixes separated by commas (44,46)</td>
</tr>
<tr>
<td></td>
<td>The Dial services by prefix dial rule in the default dial plan routes calls</td>
</tr>
<tr>
<td></td>
<td>to the assigned prefix(es) to this SBC for resolution.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a</td>
</tr>
<tr>
<td></td>
<td>prefix is routed to this SBC.</td>
</tr>
</tbody>
</table>
A postliminary is an executable script, written in the JavaScript language, that defines dial string transformations to be applied before querying the SBC.

Enabled

Lets you turn a postliminary on or off without deleting it.

Script

Type (or paste) the postliminary script you want to apply. Then click Debug this Script to open the Test Preliminary and Postliminary Scripts and test the script with various variables.

3. Click OK.

**Edit an External H.323 SBC**

You can edit an H.323 session border controller (SBC) that you previously created on your RealPresence DMA system.

SBCs to be reached by a dial rule using the Resolve to IP address action need to be configured on a per-site basis.

H.323 SBCs should be configured on a per-site basis so that calls to endpoints outside the enterprise network are routed to the SBC assigned to the originating site.

**Procedure**

1. Go to Integration > External H.323 SBCs.
2. In the Actions list, click Edit.

The following table describes the fields in the Edit External H.323 SBC dialog.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External H.323 SBC</td>
<td>Clearing this check box lets you stop using an external SBC without deleting it.</td>
</tr>
<tr>
<td>Name</td>
<td>SBC unit name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the External H.323 SBC list.</td>
</tr>
<tr>
<td>Address</td>
<td>Host name or IP address of the SBC.</td>
</tr>
<tr>
<td>Port</td>
<td>The SBC's port number. Leave set to 1720 unless you know that the unit is using a non-standard port number.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix or prefix range assigned to this SBC. Required. Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46) The Dial services by prefix dial rule in the default dial plan routes calls to the assigned prefix(es) to this SBC for resolution.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>If selected, the system strips the prefix when a call that includes a prefix is routed to this SBC.</td>
</tr>
<tr>
<td>Postliminary</td>
<td>A postliminary is an executable script, written in the JavaScript language, that defines dial string transformations to be applied before querying the SBC.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Lets you turn a postliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Script</td>
<td>Type (or paste) the postliminary script you want to apply. Then click <strong>Debug this Script</strong> to test the script with various variables.</td>
</tr>
</tbody>
</table>

3. **Click OK.**
External Skype for Business Systems

Topics:

- View External Skype for Business Systems
- Add an External Skype System
- Edit an External Skype System

When you define an external Skype for Business system, your local Polycom infrastructure gains the ability to connect to a remote Skype deployment and start or join Polycom RealConnect conferences on that system.

An external Skype system is located at a remote site and has a federated relationship with your Skype deployment.

Microsoft Skype systems configured as external SIP peers enable Polycom RealConnect conferencing for Skype deployments within your network. External Skype systems extend that capability to Skype deployments outside of your network.

When the RealPresence DMA system routes a call to an external Skype system, it uses the prefix defined for the external Skype system to determine which external Skype system to use. It then selects a Polycom MCU to host the conference and contact the external Skype system's conference auto attendant (CAA) service. The system selects an Active Directory callback contact and passes it to the selected MCU. The Skype AV MCU calls the local MCU to establish a cascade link, joining the local MCU to the conference. The MCU uses the callback contact to communicate with the local and external Skype systems, ensuring that the call is forwarded properly from the remote AV MCU to the local MCU.

Due to the external Skype system's CAA service, there may be a delay of up to 20 seconds before participants are added to the conference they dialed.

Participants can connect to Polycom RealConnect conferences hosted on external Skype systems in three ways:

- Dialing manually, using the dial string pattern

  `<Prefix><Skype_Conference_ID>@<DMA_hostname><DMA_Domain>`

- Dialing a virtual entry queue (VEQ) and entering

  `<prefix><Skype_Conference_ID>`

- Click-to-Connect, using the Polycom RealConnect Proxy service (contact Polycom Global Services for more information)

Participants using endpoints not registered to the RealPresence DMA system where the external Skype system is deployed need to manually dial these conferences using the full dial string pattern above. To make dialing simpler, you can create an address book entry on these endpoints that dials a virtual entry queue (VEQ) for a unique external Skype system. The participant then dials the address book entry and is prompted for the Polycom RealConnect conference ID. For more information on associating a VEQ with a unique external Skype system, see Shared Number Dialing.
**View External Skype for Business Systems**

You can view information about the external Skype systems that have a federated relationship with your Skype deployment.

**Procedure**

» Go to **Integrations > External Skype Systems.**

The following table describes the fields on the **External Skype Systems** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype system.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype system.</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype system to the RealPresence DMA system.</td>
</tr>
<tr>
<td>CAA dial-in SIP URI</td>
<td>The SIP address of the conference auto attendant (CAA) for the external Skype system.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template MCUs use when establishing RealConnect conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order MCUs use when establishing RealConnect conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU selection</td>
<td>The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:</td>
</tr>
<tr>
<td></td>
<td><strong>Prefer MCU in first MCU pool</strong> ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.</td>
</tr>
<tr>
<td></td>
<td><strong>Prefer MCU in first caller's site</strong> matches the MCU chosen for the call with the site that the first caller's endpoint belongs to.</td>
</tr>
<tr>
<td>Virtual entry queues</td>
<td>A list of VEQs that specify this external Skype system as a Unique external Skype system. Configured on the <strong>Service Config &gt; Conference Manager Settings &gt; Shared Number Dialing</strong> page.</td>
</tr>
</tbody>
</table>

**Add an External Skype System**

Before you add an external Skype system, ensure that Active Directory integration is enabled and at least one Microsoft external SIP peer is defined in the RealPresence DMA system.

To configure an external Skype system, you must complete the following tasks:

- Ensure the required certificates are installed (See the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide*).
- On your Active Directory server, configure Active Directory accounts for use as callback contacts (See the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide).

- Add an external Skype system configuration to the RealPresence DMA system.

- Choose an Active Directory callback contact OU on the Integrations > Microsoft Active Directory page.

- Configure a dial rule with the action Resolve to Skype Conference ID by Conference Auto Attendant.

You must create all Active Directory callback contacts within a single OU, and ensure that there are enough callback contacts in the OU for the cluster to use under heavy conferencing loads (one callback contact is used for each call to an external Skype system). There can be up to 2400 concurrent RealConnect conferences hosted on external Skype systems.

**Procedure**

1. Go to the Integrations > External Skype Systems.

2. In the Actions list, click Add.

3. In the Add External Skype System dialog, complete the editable fields, described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype system (up to 64 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype system (up to 128 characters).</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype system to the RealPresence DMA system (up to 8 characters). Callers add this prefix to the beginning of a dial string to dial in to a conference on this specific external Skype system. When the system matches dial strings against prefixes, the longest match for that dial string is used. For example, if you define an external Skype system with the prefix 2' and another with the prefix 22, the dial string 225678 results in a conference ID of 5678. If you do not specify a prefix, when the system executes a dial rule that includes this external Skype system, all dial strings will match and no further dial rules will be run. <strong>Note:</strong> Prefixes defined for external Skype systems are not listed on the Service Config &gt; Dial Plan &gt; Prefix Service page. <strong>Note:</strong> No two external Skype systems can have the same prefix, and only one external Skype system can have a blank prefix.</td>
</tr>
<tr>
<td>CAA dial-in SIP URI</td>
<td>The SIP address of the Conference Auto Attendant (CAA) for the external Skype system (up to 128 characters). The sip: URI scheme is required. <strong>Note:</strong> The RealPresence DMA system does not dial this SIP URI, but instead passes it to the MCU. Ensure the Polycom MCUs that are part of this solution are the correct version (8.6 or later) and can communicate with the external Skype system's CAA.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template MCUs should use when establishing RealConnect conferences with this external Skype system.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order MCUs should use when establishing RealConnect conferences with this external Skype system.</td>
</tr>
</tbody>
</table>
| MCU selection         | The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:  
                          **Prefer MCU in first MCU pool** ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.  
                          **Prefer MCU in first caller's site** matches the MCU chosen for the call with the site that the first caller's endpoint belongs to. |

4. Click OK.
5. Go to Integrations > Microsoft Active Directory.
6. Enable the **Callback contacts OU** field and enter the path of a container that contains the callback contact accounts you configured earlier.
   For information on how to configure callback contact accounts in Active Directory, see the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide*.

7. Click OK.
8. Go to Service Config > Dial Plan > Dial Plans to configure the RealPresence DMA system to actively use this external Skype system for calls.
9. Do one of the following:
   - If a dial rule with the action **Resolve to Skype Conference ID by Conference Auto Attendant exists**, select it and click **Edit** in the **Actions** menu.
   - If a dial rule with this action does not exist, click **Add** to create one.
10. Ensure the dial rule is enabled.
11. Move this external Skype system from the **Available external Skype systems** box to the **Selected external Skype systems** box.
12. Click OK.

**Edit an External Skype System**

In some circumstances you may need to update the configuration of an external Skype system (for example, if the remote site changes the external Skype system's settings).

**Procedure**

1. Go to the **Integrations** > **External Skype Systems**.
2. In the **Actions** list, click **Add**.
3. In the **Edit External Skype System** screen, make any changes necessary to the editable fields, described in the following table.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the external Skype for Business system (up to 64 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the external Skype for Business system (up to 128 characters).</td>
</tr>
<tr>
<td>Prefix</td>
<td>An optional prefix that identifies this external Skype for Business system to the RealPresence DMA system (up to 8 characters).</td>
</tr>
<tr>
<td></td>
<td>Callers add this prefix to the beginning of a dial string to dial a conference on this specific external Skype for Business system.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a prefix, when the system executes a dial rule that includes this external Skype for Business system, all dial strings</td>
</tr>
<tr>
<td></td>
<td>will match and no further dial rules are run.</td>
</tr>
<tr>
<td>Note:</td>
<td>No two external Skype for Business systems can have the same prefix, and only one external Skype for Business system can have a blank prefix.</td>
</tr>
<tr>
<td>CAA dial-in SIP URI</td>
<td>The SIP address of the conference auto attendant (CAA) for the external Skype for Business system (up to 128 characters). The sip: protocol</td>
</tr>
<tr>
<td></td>
<td>prefix is required.</td>
</tr>
<tr>
<td>Note:</td>
<td>The RealPresence DMA system does not dial this SIP URI, but instead passes it to the MCU. Ensure the Polycom MCUs that are part of this</td>
</tr>
<tr>
<td></td>
<td>solution are the correct version (8.6 or later) and can communicate with the external Skype for Business system's CAA. No two external Skype</td>
</tr>
<tr>
<td></td>
<td>for Business systems can have the same prefix, and only one external Skype for Business system can have a blank prefix.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template MCUs should use when establishing RealConnect conferences with this external Skype for Business system.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order MCUs should use when establishing RealConnect conferences with this external Skype for Business system.</td>
</tr>
<tr>
<td>MCU selection</td>
<td>The method for the RealPresence DMA system to use when it selects MCUs from MCU pool orders:</td>
</tr>
<tr>
<td>Prefer MCU in first MCU pool</td>
<td>Ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system</td>
</tr>
<tr>
<td></td>
<td>searches the second MCU pool for an available MCU, and so on.</td>
</tr>
<tr>
<td>Prefer MCU in first caller's site</td>
<td>Matches the MCU chosen for the call with the site that the first caller's endpoint belongs to.</td>
</tr>
</tbody>
</table>

4. Click OK.
Managing MCUs

Topics:

- MCU Management
- MCUs
- MCU Pools and Pool Orders

This section provides an introduction to managing MCUs with the Polycom RealPresence DMA system.
MCU Management

Topics:

▪ Configuring a Polycom MCU for Use with the RealPresence DMA System
▪ Configuring a Cisco MCU for Use with the RealPresence DMA System
▪ Using ISDN Gateways
▪ Bandwidth Management

The Polycom RealPresence DMA system can integrate with multipoint control units (MCUs) to enable multipoint video conferencing.

A multipoint video conference connects multiple endpoints, with all participants able to see and hear each other. The endpoints connect to an MCU, which processes the audio and video from each endpoint, and sends the conference audio and video streams back to the endpoints.

You must organize MCUs configured as conferencing resources into one or more MCU pools (logical groupings of MCUs). You can then define one or more MCU pool orders that specify the order of preference that the RealPresence DMA system uses, when it selects MCU pools.

Every conference room (virtual meeting room, or VMR) is associated with an MCU pool order. The RealPresence DMA system uses the pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs to determine which MCU will host a conference.

Configuring a Polycom MCU for Use with the RealPresence DMA System

You must configure a Polycom RealPresence Collaboration Server (MCU) to be compatible with the management functions of the RealPresence DMA system before adding it to the system.

For more detailed instructions on configuring a Polycom MCU, see the MCU product documentation.

Configure Compatible Security Settings

In enhanced security mode, the RealPresence DMA system uses only HTTPS for the conference control connection to MCUs, and you must configure your MCUs to accept encrypted connections.

When unencrypted connections are used, the MCU login name and password are sent unencrypted over the network.

Configure User Connections

By default, a RealPresence Collaboration Server or RMX MCU allows up to 20 connections per user.

We recommend not reducing this setting on the MCU (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). If you have a RealPresence DMA supercluster with three conference manager clusters and a busy conferencing environment, we recommend increasing this value to 30.
Disable Automatic Password Generation

The Automatic Password Generation feature is not compatible with the RealPresence DMA system.

On Polycom MCUs to be used with the RealPresence DMA system, disable this feature by setting the system flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_DEFAULT_LEN both to 0 (zero).

Configure SIP Settings

In a SIP signaling environment, in order for a Polycom RealPresence Collaboration Server or RMX MCU to register with the RealPresence DMA system's call server, two system flags on the MCU must be set properly:

- Set the MS_ENVIRONMENT flag to NO.
- Make sure the SIP_REGISTER_ONLY_ONCE flag is set to NO or is not present.

Register MCUs for Cascading

For cascade for size and bandwidth calls to work, you need to configure each RealPresence Collaboration Server that will be used for cascading to point to the RealPresence DMA system as the H.323 gatekeeper.

You also need to add a dial rule with the Resolve to service prefix action.

Procedure

1. Go to the RMX Manager system web interface.
2. In the RMX Management section, go to IP Network Services.
3. Double-click Default IP Service and select H.323 or H.323 & SIP as the IP Network Type.
4. Go to the Gatekeeper tab and from the Gatekeeper drop-down list, select Specify.
5. Enter either the RealPresence DMA system's IP Address or Name (as registered in the DNS).
6. Enter the IP Address or Name for a Backup Gatekeeper as needed.
7. Enter the MCU Prefix in Gatekeeper.
   The MCU uses the prefix to register with the RealPresence DMA system gatekeeper. H.323 endpoints use the prefix as the first part of their dial-in string when dialing the MCU.
8. Repeat the steps for each RealPresence Collaboration Server that will be used for cascading.

Add a Dial Rule for Cascading to MCUs

For cascade for size and bandwidth calls to work, you need to add a dial rule with the Resolve to service prefix action.

Register each RealPresence Collaboration Server that will be used for cascading to point to the RealPresence DMA system as the H.323 gatekeeper.

Procedure

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan used for H.323 signaling.
3. In Dial Rules, select the Add button.
4. Complete the fields as described in the following table:
### Field | Description
--- | ---
Description | Enter a brief description of the dial rule.
Action | Select Resolve to service prefix.
Relay Media | When selected, all media is relayed through the RealPresence DMA edge system. When not selected, all media traverses the firewall (you need to open the appropriate ports on the firewall).
Prefixed devices belong to every domain | When selected, the dial rule doesn’t require the dial string to specify a local domain when calling prefixed devices.

5. Select the Preliminary tab and enter a preliminary script if needed (optional).
6. Select OK.

## Configuring a Cisco MCU for use with the RealPresence DMA System

You need to ensure that the settings on any supported Cisco MCU are compatible with the RealPresence DMA system.

### Disable Media Port Reservations

The RealPresence DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as conferencing resources, but their Media Port Reservation feature is not supported. [ISDN Gateway Selection Process](#) on page 174

This feature must be disabled on Cisco Codian MCUs.

### Using ISDN Gateways

When a Polycom RealPresence Collaboration Server or RMX MCU functions as an ISDN gateway, each call through the gateway uses two ports, one for the ISDN side and one for the H.323 side.

The ports used for gateway calls are not available for conferences, so gateway operations may significantly reduce the available conferencing resources.

### ISDN Gateway Selection Process

When the dial string begins with a simplified ISDN gateway dialing prefix, the Polycom RealPresence DMA system chooses an ISDN gateway by applying the following steps:

1. Strip the ISDN gateway dialing prefix from the dial string, leaving the E.164 number.
2. From the in-service (not busied out or out of service) gateways, select the ones that have a profile with a matching or higher bit rate (higher bit rate can only be used for RealPresence Collaboration Server or RMX MCUs). If none, go to step 3; otherwise, go to step 4.
3. From the remaining gateways, select those with a profile bit rate lower than the requested bit rate. If none, reject the call.

4. From the remaining gateways, select those that match the country code and area code of the dialed number. If none, go to step 5; otherwise, go to step 6.

5. From the remaining gateways, select those that match the country code of the dialed number, if any.

6. From the remaining gateways, select those with a profile that has the closest bit rate. An exact match is preferred.

7. From the remaining gateways, select those that are in the same site as the calling endpoint, if any.

8. From the remaining gateways, select one using a round-robin method.

9. If the call fails because of no capacity on the selected gateway, select the next gateway left from step 8. If none, start again at step 2, (omitting the gateway that failed). If none left, reject the call.

10. If a gateway is successfully selected, assemble a dial string to send to the gateway as follows:
    \texttt{<direct
dial-in
direct
dial-in
prefix><session
profile
prefix><delimiter><E.1>}

### Bandwidth Management

For H.323 calls to a conference room (virtual meeting room, or VMR), the RealPresence DMA system can only do bandwidth management if the MCU is registered with it (in a supercluster, registered with any cluster).

If the MCU is unregistered or registered to another gatekeeper (not part of the supercluster), the bandwidth for the call isn’t counted for bandwidth management, site statistics, or the network usage report.

For the RealPresence DMA system to assign an alternate gatekeeper to an MCU, the MCU must be in a territory that has a backup RealPresence DMA system assigned to it.
MCUs

Topics:
- View MCUs
- View MCU Details
- Add an MCU
- Edit an MCU
- Add a Session Profile
- Edit a Session Profile
- Delete an MCU
- Stop Using an MCU
- Start Using an MCU
- Busy Out an MCU
- Quarantine an MCU
- Unquarantine an MCU
- Block Registrations from an MCU
- Unblock Registrations from an MCU
- View Call History

The Polycom RealPresence DMA system lists multipoint control units (MCUs) registered with the call server or that you manually add.

In a superclustered system, the list contains all MCUs in the supercluster and is the same on all systems within the supercluster. The list includes:
- MCUs that are available as a conferencing resource (enabled for conference rooms) for the RealPresence DMA system's conference manager, but not registered with the call server. Up to 64 MCUs can be enabled for VMR conference rooms.
- MCUs registered with the RealPresence DMA system's call server as standalone MCUs and/or ISDN gateways, but aren't available to the conference manager as conferencing resources.
- MCUs that are both registered with the call server and available to the conference manager as conferencing resources.

View MCUs

You can view a list of MCUs and gateways, or a combination of the two, that are available to the RealPresence DMA system.

The list displays an MCU's connection status, IP address, and additional details.

The list includes MCUs that registered with the call server or that someone manually added. If the MCU registered itself, the conference manager can use it as a standalone MCU. However, you must edit its details to enable it for conference rooms and provide additional configuration information.
Procedure

» Go to Integrations > MCUs.

The following table describes the fields in the MCU's list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status and alarm state</td>
<td>The connection, service status, and alarm state of an MCU. You can hover over an icon to see the associated status message.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the MCU.</td>
</tr>
<tr>
<td>Model</td>
<td>The type of MCU.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of software on the MCU.</td>
</tr>
<tr>
<td>IP addresses</td>
<td>The IP addresses for the MCU's management interface (M) and signaling interface (S).</td>
</tr>
<tr>
<td>Signaling type</td>
<td>The configured MCU's type of signaling: H.323, SIP, or both.</td>
</tr>
<tr>
<td>MCU pools</td>
<td>The MCU pools that use this MCU, if it's enabled as a conference manager resource.</td>
</tr>
<tr>
<td>Site</td>
<td>The site that includes the MCU.</td>
</tr>
</tbody>
</table>

View MCU Details

You can view configuration details for any managed MCU.

Procedure

1. Go to Integrations > MCUs to view the list of MCUs.
2. Select the MCU of interest.
3. Click View Details.

The screen lists configuration details for the selected MCU.

Add an MCU

You can add an MCU, gateway, or a combination of the two to enable the RealPresence DMA system to connect to the devices.

Procedure

1. Go to Integrations > MCUs.
2. Select Add.
3. Enter the MCU settings as described in the following table:
### MCU General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Name for the MCU (up to 32 characters. Don’t include the following characters: ,, ; ? : = * ).</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The types of MCUs the RealPresence DMA system supports and can connect to. For an MGC MCU, the type must be Polycom MGC gateway, even if it’s a standalone MCU.</td>
</tr>
<tr>
<td><strong>Integrate with conference manager</strong></td>
<td>When checked, the RealPresence DMA system's conference manager can use the MCU as a conferencing resource. Any Polycom MCU configured to integrate with conference manager services must be H.323 registered to the RealPresence DMA system. See the documentation for your Polycom MCUs for registration instructions.</td>
</tr>
<tr>
<td><strong>Management IP address</strong></td>
<td>The host name or IP address the RealPresence DMA system uses to log in to the MCU to use it as a conferencing resource. Polycom MCUs don't include their management IP address as a Subject Alternative Name (SAN) in their certificate signing request (CSR). Their certificates identify them by the common name (CN), which is usually the FQDN. If the Skip validation of certificates received while making outbound connections option is off in Security Settings, the CN identifies the MCU’s management interface.</td>
</tr>
<tr>
<td><strong>Admin user ID</strong></td>
<td>The Administrative user ID that the RealPresence DMA system uses to log in to the MCU.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for the administrative user ID.</td>
</tr>
<tr>
<td><strong>CIF Video ports reserved for non-DMA use</strong></td>
<td>The number of video ports on the MCU that are off-limits to the RealPresence DMA system. This number of video ports reserves some of the MCU's capacity for non-DMA use.</td>
</tr>
<tr>
<td><strong>Voice ports reserved for non-DMA use</strong></td>
<td>The number of voice ports on the MCU that are off-limits to the RealPresence DMA system. This number specifies / preserves / reserves some of the MCU's capacity for non-DMA use.</td>
</tr>
<tr>
<td><strong>Cascade-for-size reserved DIF video ports</strong></td>
<td>The number of video ports reserved for cascade links on the MCU for cascade-for-size conferences.</td>
</tr>
<tr>
<td><strong>Per-conference</strong></td>
<td>The number of video ports reserved for each cascade-for-size conference on the MCU. Subtract this number of video ports from the number of available video ports.</td>
</tr>
<tr>
<td><strong>Overall</strong></td>
<td>The number of video ports reserved for cascade-for-size cascade links on the MCU. This value is in addition to the ports reserved in Per-conference.</td>
</tr>
</tbody>
</table>
### Maximum percentage of ports in use to start a conference

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Direct Access Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable direct access</td>
<td>Check this option to enable the MCU as a directly addressed device. When enabled, the conference manager can use the MCU. Configure the signaling addresses, ports for the MCU, and the MCU's media addresses when they're selected. If you select <strong>Integrate with conference manager</strong> on the <strong>MCU General Settings</strong> tab, the system automatically populates the configuration values when it accesses the MCU.</td>
</tr>
<tr>
<td>Signaling IP for H.323</td>
<td>The address that the MCU uses for H.323 signaling. Optional field if you specify the login information for the MCU, since the system can get the address from the MCU. Required field if you don't specify the login information and enable H.323.</td>
</tr>
<tr>
<td>Signaling IP for SIP</td>
<td>The address that the MCU uses for SIP signaling. Optional field if you specify the login information for the MCU, since the system can get the address from the MCU. Required field if you don't specify the login information and enable SIP.</td>
</tr>
<tr>
<td>Transport</td>
<td>The SIP transport type to use with this MCU. If the RealPresence DMA system's security settings don't allow unencrypted connections, you must select TLS.</td>
</tr>
<tr>
<td>Add media IP addresses</td>
<td>If you specify the login settings for the MCU, the system can get media stream IP addresses from the MCU. Otherwise, enter an IP address for media streams. Then click <strong>Add</strong> to add it to the list.</td>
</tr>
<tr>
<td>Remove media IP addresses</td>
<td>Select a media address and click <strong>Remove</strong> to delete it from the list.</td>
</tr>
<tr>
<td>Direct dial-in prefix</td>
<td>The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. The Conferencing Manager can use MCUs as conferencing resources even if they don't have a prefix. If you define simplified ISDN gateway dialing prefixes, then gateways don't need a direct dial-in prefix. This way, the RealPresence DMA system can choose from a pool of available gateways.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>When checked, the system strips the prefix before routing a call that includes a prefix to this MCU.</td>
</tr>
</tbody>
</table>
**Bandwidth and Registration Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service</td>
<td>When checked, you can specify the default class of service and the bit rate limits for this MCU. If specified, calls to this MCU use its class of service or the calling endpoint's, whichever is better.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>Select the maximum bit rate for calls to this MCU.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>To manage bandwidth, select the minimum bit rate for calls to this MCU. The call drops if the minimum isn't available. The minimum bit rate that applies to a call is the higher of the MCU's bit rate and the calling endpoint's bit rate.</td>
</tr>
<tr>
<td>Permanent</td>
<td>Prevents the MCU's registration with the call server from expiring. Poly recommends that you always select this option.</td>
</tr>
<tr>
<td>Alert when MCU unregisters</td>
<td>If you check this option but don’t check the Permanent option, an alert displays when the MCU unregisters from the call server or its registration expires.</td>
</tr>
</tbody>
</table>

**ISDN Gateway Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ISDN GW function</td>
<td>When checked, you can select the MCU as an ISDN gateway device and configure gateway session profiles. Gateway session profiles specify the bandwidth parameters for the ISDN connection to the MCU. For ISDN gateway calls to the MCU's direct dial-in prefix, the caller specifies the session profile prefix in the dial string: <code>&lt;direct dial-in prefix&gt;&lt;session profile prefix&gt;&lt;delimiter&gt;&lt;E.164 number&gt;</code> For calls to simplified ISDN gateway dialing prefixes, the RealPresence DMA system selects the MCU/gateway and its session profile.</td>
</tr>
<tr>
<td>Copy from entry for ISDN gateway</td>
<td>From the drop-down menu, you can select the delimiter and session profiles from another ISDN gateway to copy them instead of entering them. This is useful for MGC devices since all cards support the same gateway configuration, even though you must register each ISDN network card separately.</td>
</tr>
<tr>
<td>Dial string delimiter</td>
<td>The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Session profile prefix table | Lists the defined session profile prefixes. A session profile prefix is a numeric dial string that specifies a bit rate for the call and the protocols it supports.

You can add a session profile and edit or delete a selected profile. You can’t change or delete session profiles that the MCU/gateway used to register.

Postliminary

Field | Description
--- | ---
Enabled | A postliminary is an executable script, written in the JavaScript language, that defines dial transformations to apply before routing the call to the MCU/gateway.

This check box enables you to turn a postliminary script on or off without deleting it.

Script | Type (or paste) the postliminary script you want to apply. Then click **Debug this Script** to open the **Script Debugging** window and test the script with different variables.

4. Click **OK**.

The new MCU appears in the **MCUs** list. If the MCU is a conferencing resource, it's placed into service.

5. If the MCU is a conferencing resource, add it to the desired MCU pool(s).

**Edit an MCU**

You can edit the settings of an MCU that isn’t in use.

If you need to edit the login information for the MCU (**Management IP**, **Admin ID**, or **Password**), you must first stop using the MCU by terminating existing calls and conferences, or busy it out and wait for existing calls and conferences to end.

**Procedure**

1. On the Dashboard, verify that there are no calls and conferences on the MCU you want to edit.
2. Go to **Integrations > MCUs**.
3. Select the MCU to edit and click **Edit**.
4. Edit the fields in the following table as required.

**MCU General Settings**

Field | Description
--- | ---
Name | Name for the MCU (up to 32 characters; must not include any of the following: `; " ? : = `).
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Lists the types of MCUs the system supports. This must be set to the correct MCU type in order for the RealPresence DMA system to connect to it. For an MGC MCU, this field must be set to Polycom MGC gateway, even if it's being used as a standalone MCU.</td>
</tr>
<tr>
<td>Integrate with conference manager</td>
<td>When checked, the MCU can be used as a conferencing resource for the RealPresence DMA system's conference manager. Any MCU of the type Polycom MCU that you configure to integrate with conference manager services must always be H.323 registered to the RealPresence DMA system. For instructions on H.323 registering a Polycom MCU to the RealPresence DMA system, see the documentation for your specific Polycom MCUs.</td>
</tr>
<tr>
<td>Management IP address</td>
<td>The host name or IP address the RealPresence DMA system uses to log in to the MCU to use it as a conferencing resource. Polycom MCUs don't include their management IP address in the Subject Alternate Name (SAN) field of the CSR (certificate signing request), so their certificates identify them only by the common name (CN). Therefore, if Skip validation of certificates received while making outbound connections is off in Security Settings, the MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by IP address.</td>
</tr>
<tr>
<td>Admin user ID</td>
<td>The Administrative user ID that the RealPresence DMA system uses to log in to the MCU.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the administrative user ID.</td>
</tr>
<tr>
<td>CIF Video ports reserved for non-DMA use</td>
<td>The number of video ports on the MCU that are off-limits to the RealPresence DMA system. This number of video ports reserves some of the MCU's capacity for non-DMA use.</td>
</tr>
<tr>
<td>Voice ports reserved for non-DMA use</td>
<td>The number of voice ports on the MCU that are off-limits to the RealPresence DMA system. This number (<em>specifies / preserves / reserves</em>) some of the MCU's capacity for non-DMA use.</td>
</tr>
<tr>
<td>Cascade-for-size reserved DIF video ports</td>
<td>The number of video ports on the MCU that is reserved for cascade links when you create a conference on the MCU that has cascade-for-size enabled.</td>
</tr>
<tr>
<td>Per-conference</td>
<td>The number of video ports on the MCU reserved for cascade links. For each cascade-for-size conference on the MCU, this number of video ports is subtracted from the number of video ports available for participants.</td>
</tr>
<tr>
<td>Overall</td>
<td>The number of video ports reserved for cascade-for-size cascade links on the MCU. This is in addition to the Per-conference value.</td>
</tr>
</tbody>
</table>
## Direct Access Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable direct access</td>
<td>This enables the MCU to be used as a directly addressed device, independent of whether or not the conference manager uses the MCU. The signaling addresses, ports for the MCU, and the MCU's media addresses must be configured when they're selected. If the setting <strong>Integrate with conference manager</strong> is selected on the <strong>MCU General Settings</strong> tab, the system will automatically populate these values when it accesses the MCU.</td>
</tr>
<tr>
<td>Signaling IP for H.323</td>
<td>The address that the MCU uses for H.323 signaling. If you specify the login information for the MCU, this field is optional since the system can get the address from the MCU. If not, and H.323 is enabled, this field is required.</td>
</tr>
<tr>
<td>Signaling IP for SIP</td>
<td>The address that the MCU uses for SIP signaling. If you specify the login information for the MCU, this field is optional since the system can get the address from the MCU. If not, and SIP is enabled, this field is required.</td>
</tr>
<tr>
<td>Transport</td>
<td>The SIP transport type to use with this MCU. If the RealPresence DMA system's security settings don't allow unencrypted connections, this must be TLS.</td>
</tr>
<tr>
<td>Add media IP addresses</td>
<td>If you specify the login settings for the MCU, the system can get media stream IP addresses from the MCU. If you don't specify login settings, enter an IP address for media streams and click <strong>Add</strong> to add it the list.</td>
</tr>
<tr>
<td>Remove media IP addresses</td>
<td>Select a media address and click <strong>Remove</strong> to delete it from the list.</td>
</tr>
<tr>
<td>Direct dial-in prefix</td>
<td>The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. The Conferencing Manager can use MCUs as conferencing resources even if they don't have a prefix. If you define simplified ISDN gateway dialing prefixes, then gateways don't need a direct dial-in prefix. This way, the RealPresence DMA system can choose from a pool of available gateways.</td>
</tr>
<tr>
<td>Strip prefix</td>
<td>When checked, the system strips the prefix when a call that includes a prefix route to this MCU.</td>
</tr>
</tbody>
</table>

## Bandwidth and Registration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service</td>
<td>When checked, you can specify the default class of service and the bit rate limits for this MCU. If specified, calls to this MCU use its class of service or the calling endpoint's, whichever is better.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum bit rate (kbps)</strong></td>
<td>Select the maximum bit rate for calls to this MCU.</td>
</tr>
<tr>
<td><strong>Minimum downspeed bit rate (kbps)</strong></td>
<td>To manage bandwidth, select the minimum bit rate to which calls to this MCU can be downspeeded. The call is dropped if the minimum isn’t available. The minimum bit rate that applies to a call is the higher of the MCU's and the calling endpoint's.</td>
</tr>
<tr>
<td><strong>Permanent</strong></td>
<td>If checked, this option prevents the MCU's registration with the call server from expiring. This option should always be selected.</td>
</tr>
<tr>
<td><strong>Alert when MCU unregisters</strong></td>
<td>If checked, this option triggers an alert if the MCU unregisters from the call server or its registration expires (if the Permanent check box isn’t selected).</td>
</tr>
</tbody>
</table>

### ISDN Gateway Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable ISDN GW function</strong></td>
<td>When checked, this option makes the MCU available for selection as an ISDN gateway device and enables the configuration of gateway session profiles. Gateway session profiles indicate the bandwidth parameters for the ISDN connection to the MCU. Session profiles can be used for the following calls:</td>
</tr>
<tr>
<td></td>
<td>• ISDN gateway calls to the MCU's direct dial-in prefix. In this case, the caller specifies the session profile prefix in the dial string: &lt;direct dial-in prefix&gt;&lt;session profile prefix&gt;&lt;delimiter&gt;&lt;E.164 number&gt;</td>
</tr>
<tr>
<td></td>
<td>• Calls to simplified ISDN gateway dialing prefixes. In this case, the RealPresence DMA system selects the MCU/gateway and its session profile.</td>
</tr>
<tr>
<td><strong>Copy from entry for ISDN gateway</strong></td>
<td>From the drop-down list, you can select the delimiter and session profiles from another ISDN gateway to copy them instead of entering them. This is useful for MGC devices since all cards support the same gateway configuration, even though each ISDN network card must be registered separately.</td>
</tr>
<tr>
<td><strong>Dial string delimiter</strong></td>
<td>The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number.</td>
</tr>
</tbody>
</table>
Add a Session Profile

You can add a session profile to the ISDN gateway for an MCU that’s enabled as an ISDN gateway device.

Procedure
1. Go to Integrations > MCUs.
2. Select an MCU that’s enabled as an ISDN gateway device.
3. Click Edit.
4. Select ISDN Gateway Settings.
5. Select Enable ISDN GW Function.
6. Click Add.
7. Complete the fields to add a session profile as described in the following table:
Select the protocols for this profile. Only H.320 and PSTN are relevant when adding a profile. The other protocols have check marks if the gateway specified them when registering.

8. Click OK.

The new session profile displays in the list.

Edit a Session Profile

You can edit a session profile that you added.

You can't edit a session profile that the MCU used to register to the RealPresence DMA system.

Procedure

1. Go to Integrations > MCUs.
2. Select the MCU with the session profile to edit and click Edit.
3. Select ISDN Gateway Settings.
4. Select a session profile from the list.
5. Click Edit.
6. Revise the fields in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session profile prefix</td>
<td>Numeric dial string prefix for this profile.</td>
</tr>
<tr>
<td>Bit rate</td>
<td>Bit rate of calls using this profile.</td>
</tr>
<tr>
<td>H.320 PSTN H.323 SIP</td>
<td>Select the protocols for this profile. Only H.320 and PSTN are relevant when editing a profile you added. The other protocols have check marks if the gateway specified them when registering.</td>
</tr>
</tbody>
</table>

7. Click OK.

Delete an MCU

You can delete an MCU to remove it as an available conferencing resource.

You can't delete an MCU if either of the following conditions is true:

- **The MCU is hosting one or more conferences.**
  - You can delete the MCU after you busy it out and wait for all conferences to end.
- **The MCU is registered with the call server.**
  - You can delete the MCU after you unregister it.
Procedure
1. On the Dashboard, verify that there are no calls and conferences on the MCU you want to delete.
2. Go to Integrations > MCUs.
3. Select the MCU to delete and click Delete.
4. Click Yes to confirm.

Stop Using an MCU
You can immediately stop the RealPresence DMA system from using one or more MCUs as conferencing resources or ISDN gateways.

When you stop using an MCU, the RealPresence DMA system immediately terminates all H.323 calls and conferences on the MCU. For SIP calls, the system migrates the calls to in-service MCUs that have available capacity. The RealPresence DMA system won’t select MCUs you have stopped using for any future conferences and simplified ISDN dialing calls.

Note that this command terminates the RealPresence DMA system’s use of an MCU, but the MCU can continue to accept any calls from other sources.

Procedure
1. Go to Integrations > MCUs.
2. Select the MCU to stop using and click Stop Using.
3. Click Yes to confirm.

Start Using an MCU
You can put an MCU back in service again for conferencing and simplified gateway dialing if it has been stopped or busied out.

Procedure
1. Go to Integrations > MCUs.
2. Select the stopped or busied-out MCU to start using again and click Start Using.

Busy Out an MCU
The RealPresence DMA system stops creating new conferences on MCUs that you busy out, but allows existing conferences to continue and accepts new calls to those conferences.

The system also excludes busied-out MCUs from consideration for simplified ISDN dialing calls.

Procedure
1. Go to Integrations > MCUs.
2. Select one or more MCUs to busy out and click Busy Out.
3. Click Yes to confirm.
Quarantine an MCU

A quarantined MCU can register (or remain registered) with the call server, but can’t make or receive calls.

Quarantining is intended only for MCUs that are registered with the RealPresence DMA system's call server as standalone MCUs and/or ISDN gateways, but are not available to the conference manager as conferencing resources.

Procedure

1. Go to Integrations > MCUs.
2. In the MCUs list, select the MCU to quarantine and click Quarantine.

Unquarantine an MCU

If you quarantine one or more MCUs, the Unquarantine option displays in the system web interface.

When you unquarantine an MCU that is registered with the RealPresence DMA call server, the MCU can make or receive calls again.

Procedure

1. Go to Integrations > MCUs.
2. Select the MCU to unquarantine and click Unquarantine.

Block Registrations from an MCU

You can prevent one or more MCUs from registering with the call server.

Procedure

1. Go to Integrations > MCUs.
2. Select the MCU to prevent from registering with the call server and click Block Registrations.

Unblock Registrations from an MCU

If one or more MCUs are blocked, the Unblock Registrations option displays in the system web interface.

You can enable one or more MCUs to register with the RealPresence DMA call server by unblocking them.

Procedure

1. Go to Integrations > MCUs.
2. Select the MCU to unblock from registering with the call server and click Unblock Registrations.

View Call History

An MCU's call history report includes the following call details:
- Originator
- Destination
- Dial string
- Start time
- End time
- Ingress cluster
- Call ID

**Procedure**

1. Go to **Integrations > MCUs**.
2. Select the **MCU** with the call history you want to view.
3. Under **Actions**, click **View Call History**.
   The call history report displays.
MCU Pools and Pool Orders

Topics:

- **MCU Selection Process**
- **MCU Availability and Reliability Tracking**
- **Working with MCU Pools**
- **Working with MCU Pool Orders**

The RealPresence DMA system requires you to create uses MCU pools, or logical groupings of media servers, before you can use an MCU as a conferencing resource.

You can determine how to group MCU pools. For example, you can base an MCU pool on location, capability, or some other factor.

After creating the MCU pools you need, you can configure a Pool Order. A pool order contains one or more MCU pools and specifies the order of preference in which the RealPresence DMA system will use the pools. The RealPresence DMA system uses the pools to which an MCU belongs, and the pool order(s) to which a pool belongs, to determine which MCU will host a conference.

Every conference room (VMR) is associated with an MCU pool order by direct assignment, through the user's enterprise group membership, or from the system default).

**Note:** The RealPresence DMA system doesn't use MCU pools and pool orders to select an ISDN gateway for simplified gateway dialing.

You can use various criteria for organizing MCUs into pools, depending on how you want the MCU resources allocated for conferencing. For instance:

- Assign all MCUs in a specific site or domain to a pool. Then, assign a pool order to all users in that site or domain (via group membership), ensuring that their conferences are preferentially routed to MCUs in that pool.
- Assign one or more MCUs to a pool to be used only by executives, and assign that pool to a pool order associated only with those executives' conference rooms.
- Assign MCUs with special capabilities to a pool and assign that pool to a pool order associated only with custom conference rooms requiring those capabilities.

**Related Links**

- [View Conference Rooms](#) on page 458
- [Add a Conference Room for a User](#) on page 459
- [Edit a Conference Room for a User](#) on page 465
- [Assign Conference Properties to a Group](#) on page 479
- [Edit a User](#) on page 453
- [User Roles](#) on page 443
MCU Selection Process

The RealPresence DMA system can assess only the resources that an MCU currently has available. The system can’t assess the resources that have been scheduled for future use.

In Conference Settings, when the Default MCU selection algorithm field is set to Prefer MCU in first caller’s site, the system will match the MCU chosen for the call with the site that the first caller’s endpoint belongs to.

In Conference Templates, Polycom MCU General Settings, the Cascade for size option enables conferences using that template to span Polycom MCUs to support conference sizes larger than a single MCU can accommodate.

If you select Cascade for Size and Prefer MCU in first caller’s site (the Default MCU selection algorithm in Conference Settings), the rules for Cascade for size take precedence over the rules for Prefer MCU in first caller’s site during MCU selection. If a conference starts on an MCU with insufficient ports reserved for Cascade for size, then the conference will never cascade.

The RealPresence DMA system assigns an MCU for a user's conference by applying the following rules in order:

1. Select the MCU pool order:
   a. Use the pool order directly assigned to the user's conference room.
   b. If none, use the highest priority pool order associated with any group to which the user belongs.
   c. If none, use the system default.

2. Select the first MCU pool in the MCU pool order.

3. Select the best MCU in the MCU pool, based on how well their capabilities fulfill the user's needs in the following respects:
   - MCU has RealPresence Collaboration Server or RMX profile required by user's conference template.
   - MCU has IVR service required by user's conference template.
   - MCU has recording capability required by user's conference template.
   - MCU supports WebRTC clients.
   - MCU supports SVC conferencing.
   - MCU supports cascaded conferences with both on-premises and external Skype for Business AVMCUs.

4. If there are multiple MCUs that are equally capable, select the least used, as determined by the following formula:

   \[
   \text{availability} = 1 - \frac{(\text{used}_{\text{video}} \text{ ports} + \text{used}_{\text{audio}} \text{ ports})}{(\text{total}_{\text{video}} \text{ ports} + \text{total}_{\text{audio}} \text{ ports})}
   \]

5. If no MCUs in the selected MCU pool have capacity, select the next MCU pool in the pool order and return to step 3.

6. If no MCUs are available in any of the MCU pools in the pool order:
• If fallback is enabled, select the best MCU available to the RealPresence DMA system, based on the system's capability algorithm.
• If fallback isn’t enabled, reject the call.

MCU Availability and Reliability Tracking

To minimize the number of failed calls, the RealPresence DMA system employs mechanisms for detecting and handling MCU availability and reliability issues:

• If it can’t reach an MCU’s management interface, the RealPresence DMA system won’t route calls to that MCU.
• If an MCU reports zero capacity via its management interface, the RealPresence DMA system won’t route calls to that MCU.
• When calls to a specific MCU fail, the RealPresence DMA system reduces the MCU’s reliability score, causing it to be selected less frequently than other MCUs.

An MCU’s reliability depends on the number of consecutive failed calls. As that number increases, the RealPresence DMA system treats a growing percentage of the MCU's ports as if they were in use. Since the RealPresence DMA system selects the least used of the capable MCUs in its pool, the likelihood that an MCU with failures will be chosen for the next call declines rapidly (depending on the number of consecutive failed calls and the remaining capacity in the MCU pool).

<table>
<thead>
<tr>
<th>Consecutive Failed Calls</th>
<th>Percentage of Ports Assumed to be in Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>24%</td>
</tr>
<tr>
<td>2</td>
<td>43%</td>
</tr>
<tr>
<td>3</td>
<td>56%</td>
</tr>
<tr>
<td>4</td>
<td>67%</td>
</tr>
<tr>
<td>5</td>
<td>74%</td>
</tr>
<tr>
<td>6</td>
<td>80%</td>
</tr>
<tr>
<td>7</td>
<td>84%</td>
</tr>
<tr>
<td>8</td>
<td>88%</td>
</tr>
<tr>
<td>9</td>
<td>90%</td>
</tr>
</tbody>
</table>

Every 30 minutes, the reliability score of the MCU is increased so that it won't be permanently removed from the pool due to failures in the past. To avoid trying the MCU every 30 minutes, monitor the RealPresence DMA system and administratively take the MCU out of service.

• By increasing the number of MCUs in the pool or increasing their capacity, you can decrease the usage of the working MCUs during a failover scenario. So, for example, if you want to avoid routing any more calls to an MCU after two consecutive failed calls, provide enough excess capacity that the remaining MCUs never all reach 43% port usage during a failure.
Working with MCU Pools

After you manually add an MCU to your RealPresence DMA system, you need to add it to an MCU pool so it can be used as a conference resource.

Conferencing resources can be assigned for use in conferences. Note that MCUs that are registered to the RealPresence DMA system (not added by you), cannot be added to an MCU pool.

View MCU Pools

You can view a list of MCU pools you have created.

Procedure

» Go to Service Config > Conference Manager Settings > MCU Pools.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the pool, such as the geographic location of the MCUs it contains.</td>
</tr>
<tr>
<td>MCUs</td>
<td>The MCUs that are in the pool.</td>
</tr>
</tbody>
</table>

Add an MCU Pool

You can define a new MCU pool in the RealPresence DMA system.

Procedure

1. Go to Service Config > Conference Manager Settings > MCU Pools.
2. Click the Add button.
3. Enter a name and description for the MCU pool.
4. Select the MCUs to include in the pool by using the arrow buttons to move MCUs from the Available MCUs list to the Selected MCUs list.
5. If applicable, select the ContentConnect Systems tab and select the Polycom ContentConnect systems to include in the pool by using the arrow buttons to move systems from the Available ContentConnect Systems list to the Selected ContentConnect Systems list.
6. Click OK.

Edit an MCU Pool

You can edit an existing MCU pool at any time.
Procedure

1. Go to Service Config > Conference Manager Settings > MCU Pools.
2. In the MCU Pools list, select a pool and click the Edit button.
3. Change the name or description for the MCU pool as needed.
4. Use the arrow buttons to move MCUs between the Available MCUs list and the Selected MCUs list.
5. If applicable, select the ContentConnect Systems tab and use the arrow buttons to move Polycom ContentConnect systems between the Available ContentConnect Systems list and the Selected ContentConnect Systems list.
6. Click OK.

The changes you made display in the MCU Pools list.

Delete an MCU Pool

You can delete an MCU pool if it is no longer needed.

Procedure

1. Go to Service Config > Conference Manager Settings > MCU Pools.
2. Select the MCU pool you want to remove.
3. Click the Delete button.

If the pool is included in one or more pool orders, a warning displays with information about the consequences of deleting the pool.
4. Click Yes to confirm the deletion.

Working with MCU Pool Orders

A pool order contains one or more MCU pools and specifies the order of preference in which the pools are used.

Every conference room (VMR) is associated with an MCU pool order in one of the following ways:

- By direct assignment.
- Via the user’s enterprise group membership.
- From the system default.

The pool(s) to which an MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used to host a conference.

You can configure an MCU pool order to fall back to any available MCU if no MCU within the pool order’s selected pools is available to host a conference. When the system selects an MCU based on the Fall back to any available MCU setting, the selected MCU is considered to be a member of the pool order.

MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing.

Related Links

Edit a Conference Room for a User on page 465
Naming Conventions for Pool Orders

If you have a Polycom RealPresence Resource Manager system that is configured to schedule conferences on the RealPresence DMA system's conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for use by the RealPresence Resource Manager system.

The pool orders should be named in such a way that:
- They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
- Users will understand that they should choose one of the RealPresence Resource Manager system's pool orders.

View MCU Pool Orders

You can view MCU pool orders.

In a superclustered system, this list is the same on all clusters in the supercluster.

Procedure

» Go to Service Config > Conference Manager Settings > MCU Pool Orders.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority ranking of the pool order.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
<tr>
<td>MCU Pools</td>
<td>The MCU pools that are in the pool order.</td>
</tr>
<tr>
<td>Fallback</td>
<td>Indicates whether this pool order is configured to use any available MCU if none are available in its pools.</td>
</tr>
</tbody>
</table>

Add an MCU Pool Order

You can add an MCU pool order to specify the order of preference in which the RealPresence DMA system uses existing MCU pools.

Procedure

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. In the Actions list, click Add.
3. In the Add MCU Pool Order window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available MCU pools</td>
<td>Lists the MCU pools available to the system.</td>
</tr>
<tr>
<td>Selected MCU pools</td>
<td>Lists the pools included in the pool order in their priority order. The left/</td>
</tr>
<tr>
<td></td>
<td>right arrow buttons move pools in and out of the list. The up/down</td>
</tr>
<tr>
<td></td>
<td>arrow buttons change the priority rankings of the pools.</td>
</tr>
<tr>
<td>Fall back to any available MCU</td>
<td>Indicates whether this pool order will use any available MCU if there</td>
</tr>
<tr>
<td></td>
<td>are no available MCUs in this pool order's pools.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

The new MCU pool order appears in the **MCU Pool Orders** list. The MCU pools included in the pool order are displayed.

## Edit an MCU Pool Order

Once you create an MCU pool order, you can change it at any time.

### Procedure

1. Go to **Service Config > Conference Manager Settings > MCU Pool Orders**.
2. In the **MCU Pool Orders** list, select the pool order, and in the **Actions** list, click **Edit**.
3. In the **Edit MCU Pool Order** dialog, edit the following fields as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the MCU pool order.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the pool order.</td>
</tr>
<tr>
<td>Available MCU pools</td>
<td>Lists the MCU pools available to the Polycom RealPresence DMA system.</td>
</tr>
<tr>
<td>Selected MCU pools</td>
<td>Lists the pools included in the pool order in their priority order. The left/</td>
</tr>
<tr>
<td></td>
<td>right arrow buttons move pools from one list to the other. The up/down</td>
</tr>
<tr>
<td></td>
<td>arrow buttons change the priority rank of the selected pool.</td>
</tr>
<tr>
<td>Fall back to any available MCU</td>
<td>Indicates whether this pool order is set to fall back to any available</td>
</tr>
<tr>
<td></td>
<td>MCU if there are no available MCUs in its pools.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

The changes you made display in the list of **MCU Pool Orders** list.

## Edit the Priority Ranking of a Pool Order

You can modify the priority in which a pool order is used.

### Procedure

1. Go to **Service Config > Conference Manager Settings > MCU Pool Orders**.
2. Select the MCU you want to change.
3. Click the **Move Up** or **Move Down** arrow buttons to change the position of the MCU is in list.
Delete an MCU Pool Order

If an MCU pool order is no longer needed, you can delete it from the system.

Procedure

1. Go to Service Config > Conference Manager Settings > MCU Pool Orders.
2. In the list of MCU pool orders list, select the pool order to delete.
3. Click the Delete button.
4. Click Yes to confirm the deletion.
Integration with Other Services

Topics:

- Polycom RealPresence DMA System Edge to Core Integration
- Microsoft Active Directory Integration
- Microsoft Exchange Server Integration
- Microsoft Skype for Business Integration
- RealPresence Resource Manager Integration
- Polycom ContentConnect Integration
- VPN Tunnel Settings

This section provides an introduction to integrating the Polycom RealPresence DMA System with other services on your network.
Polycom RealPresence DMA System
Edge to Core Integration

Topics:

- Run the RealPresence DMA Edge Wizard

A RealPresence DMA edge system can be configured to integrate with a RealPresence DMA core system.

It's recommended that you run the DMA Edge Wizard to configure the edge system automatically, but you can also configure it manually.

After you initially set up a RealPresence DMA edge system and core system on your network, you can use the DMA Edge Wizard to create all the necessary connections for the edge system and core system to communicate. You shouldn't use the wizard if you deploy a combination-configured system or upgrade a Polycom RealPresence Access Director system to a RealPresence DMA system.

You can also use the DMA Edge Wizard to configure two edge systems in VPN tunnel mode.

Run the RealPresence DMA Edge Wizard

When you run the DMA Edge Wizard on an edge-configured RealPresence DMA system, the wizard creates the default connections required for communication with a core-configured RealPresence DMA system.

The connections include an external SIP peer, an external H.323 gatekeeper, and registration sharing. The wizard also configures the default dial rules and access control list (ACL) to facilitate communication.

Procedure

1. Go to Integrations > DMA Edge Wizard.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management host name of core DMA</td>
<td>The FQDN or IP address of the network interface assigned to management on the core RealPresence DMA system.</td>
</tr>
<tr>
<td>Core DMA user name</td>
<td>The administrator user name used to log into the management interface of the core system.</td>
</tr>
<tr>
<td>Core DMA user password</td>
<td>The administrator password used to log into the management interface of the core system.</td>
</tr>
<tr>
<td>Core DMA uses the same IP address for management and signaling</td>
<td>If not selected, enter the <strong>Signaling host name of Core DMA</strong>, which is the FQDN or IP address of the network interface assigned to signaling on the core system. If selected, the system automatically populates the <strong>Signaling host name of Core DMA</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Signaling host name of core DMA</td>
<td>The FQDN or IP address of the network interface assigned to signaling on the core RealPresence DMA system.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Core DMA uses the same IP address for management and signaling</strong>, the system automatically populates this field.</td>
</tr>
<tr>
<td>External SIP peer port</td>
<td>The SIP signaling port number of the external SIP peer that the wizard creates.</td>
</tr>
<tr>
<td>External SIP peer transport type</td>
<td>The transport protocol to use when contacting the external SIP peer.</td>
</tr>
<tr>
<td>External H.323 gatekeeper RAS port</td>
<td>The RAS port number of the external H.323 gatekeeper that the wizard creates.</td>
</tr>
<tr>
<td>Maximum number of simultaneous calls</td>
<td>The maximum number of simultaneous calls your edge system supports.</td>
</tr>
<tr>
<td></td>
<td>The wizard assigns three SIP and three H.323 dynamic ports for the maximum number of calls you specify. For example, if you enter 500 as the maximum number of simultaneous calls, the wizard assigns 1500 dynamic ports for SIP calls and 1500 dynamic ports for H.323 calls.</td>
</tr>
</tbody>
</table>

3. **Click Next.**

The wizard displays the signaling **IP address** on the core system.

4. Click the **Add** button to enter additional IP addresses if necessary:
   - For HA systems, add the virtual IP address for an active-passive pair or add the two virtual IP addresses for an active-active pair.
   - For superclusters, add the signaling IP addresses of each core system.

5. Click **OK** to create the default connections between the edge system and the core system.
   - Note the items and settings that the DMA Edge Wizard created.

6. **Click OK.**

7. Go to the core system and do one of the following:
   - Create or edit a site and configure the same settings that the DMA Edge Wizard created on the edge system (external SIP peer, external H.323 gatekeeper, default dial rules, and default ACL).
   - Configure the settings manually without creating a site.
Microsoft Active Directory Integration

Topics:

- Integrate with Active Directory
- Understanding Base DN
- Adding Passcodes for Enterprise Users
- Active Directory Cache Refresh Frequency
- Orphaned Groups and Users
- About the System's Directory Queries
- View the Active Directory Page

When you integrate the RealPresence DMA system with your Microsoft Active Directory, the enterprise users (Active Directory members) become Conferencing Users in the RealPresence DMA system.

Each enterprise user is (optionally) assigned a conference room or virtual meeting room (VMR). The conference room IDs are typically generated from the enterprise users' phone numbers.

Once integrated with Active Directory, the RealPresence DMA system accesses the directory under the following circumstances:

- Nightly, to update the user and group information in its cache.
- Whenever you force a cache refresh using the Update button.
- To authenticate login passwords.
- To create or delete Polycom conference contacts whenever a publishable VMR is created or deleted (only if the RealPresence DMA system is integrated with Microsoft Lync 2013 or Skype for Business and contact creation is enabled).

In a super-clustered environment, one cluster is responsible for integrating with the Active Directory and updating the cache daily, and the cache is available to all clusters through the replicated shared data store. The other clusters only connect to the Active Directory to authenticate user credentials.

Related Links
Set Up Security
Integrate with Active Directory on page 201

Integrate with Active Directory

When you integrate your RealPresence DMA system with Microsoft Active Directory, you should know approximately how many enterprise users you expect the system to retrieve.

If you have a RealPresence Resource Manager system, be aware that the machine account used for Active Directory integration by the RealPresence Resource Manager system and the service account used for Active Directory integration by the RealPresence DMA system have different requirements. Don't use the same account for both purposes.

If you use Active Directory attributes that are not replicated across the enterprise through the Global Catalog server mechanism, the system must query each domain for the data. Make sure that the whitelist...
for the service account that the RealPresence DMA system uses is correct and that it can connect to all the LDAP servers in each domain.

**Note:** Unless the **Allow unencrypted connections to the Active Directory** security option is enabled, the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system’s management interface. The Microsoft Active Directory server must be configured to trust the CA.

**Procedure**

1. In Windows Server, add the service account (read-only user account) that the RealPresence DMA system will use to read the Active Directory and configure the account as follows:
   - User cannot change password.
   - Password never expires.
   - User can only access services on the domain controllers and can’t log in anywhere. If you’re integrating the RealPresence DMA system with Lync 2013 or Skype for Business and plan to use the automatic conference contact creation feature, the service account you create here should have full permissions to add, change, and delete entries in the OU where the conference contacts are stored, along with full administrative permissions for Lync or Skype administration to manipulate these contacts.

2. In the RealPresence DMA system, replace the default local administrative user with your own user account that has the same user roles.

3. Log in to the RealPresence DMA system as the local user you created in the preceding step and go to **Integrations > Microsoft Active Directory**.

4. Check the **Integrate with Enterprise Directory Server** option and complete the information in the **General Integration Settings** section.
   - Do one of the following:
     - Unless you have a single domain environment and no global catalog, select **Auto-discover** and enter the DNS domain name.
     - Select **IP Address or FQDN** and enter the appropriate value.
       Don’t use the IP address or host name option in a multi-domain environment. If you must do so, enter the host name or IP address of a specific global catalog server, not the DNS domain name.
   - For **Domain > Enterprise directory user ID**, enter the domain and user ID of the account that you created previously.
   - For **Enterprise directory user password**, enter the password of the account you created previously.
   - Leave **Security Level** set to the default **Automatic**.
   - Edit the **User LDAP filter** expression only if you understand LDAP filter syntax (see RFC 2254) and know what changes to make.
   - Leave **Base DN** set to the default **All Domains**.

5. Complete the information in the **Cache Refresh** section.
   - For **Number of cache refreshes per day**, specify how many times per day the RealPresence DMA should check the Active Directory for changes.
   - For **Time of day to refresh cache**, specify the time of day the RealPresence DMA system should check the Active Directory for changes.
c. For **Territory for cache refresh**, select the territory whose cluster should perform the integration and daily updates.

6. To generate conference room IDs for the enterprise users, complete the **Enterprise Conference Room ID Generation** section.

   Skip this step if you don’t want the system to create conference rooms (virtual meeting rooms) for the enterprise users.

   a. For **Directory attribute**, specify the Active Directory attribute from which to generate unique room IDs, typically phone numbers or employee ID numbers.

   b. If necessary, edit the contents of the **Characters to remove** field.

      If you use phone numbers, the default contents of this field should be adequate to ensure a numeric room ID.

   c. Specify the **Maximum characters used**.

      After the RealPresence DMA system removes the characters specified in the **Characters to remove** setting, it removes characters in excess of the number specified for the **Maximum characters used** setting from the beginning of the string.

      **Note:** Don’t update the **Enterprise Chairperson and Conference Passcode Generation** section now. Once the system is integrated successfully, you can add passcode support.

7. If your environment uses external Lync or Skype for Business systems, enable the **Callback contacts OU** field and enter the path of a container that contains callback contact accounts for use with external Skype systems.

   For information on how to configure callback contact accounts in Active Directory, see the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide*.

8. Click **Update**.

   After a short time, the system confirms that Active Directory configuration has been updated.

9. Note the time and click **OK**.

10. To restrict the RealPresence DMA system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain), repeat steps 4 to step 8, selecting the value you want from those now available in the **Base DN** list.

11. Check the **Total users/rooms** and **Conference room errors** values.

    If the numbers are significantly different from what you expected, you'll need to investigate after you complete the next step (you must be logged in as an enterprise user to investigate further).

12. Set up your enterprise account and secure the service account:

    a. Log out and log back in using the service account you created in step 1.

       You must be logged in with an Active Directory user account to see other enterprise users. Use the service account user ID created in the initial step.

    b. Go to **User > Users**, clear the **Local users only** check box, locate your named enterprise account, and give it Administrator privileges.

    c. Log out and log back in using your named enterprise account.

    d. Secure the service account by removing all user roles and marking it disabled in the RealPresence DMA system (not in the Active Directory) so that this account cannot be used for conferencing or for logging in to the RealPresence DMA system management interface.
13. If the **Total users/rooms** values were significantly different from what you expected, try to determine the reason and fix it:

   a. Go to **User > Users** and perform some searches to determine which enterprise users are available and which are not.

   b. If there are many missing or incorrect users, consider whether changes to the LDAP filter can correct the problem or if there is an issue with the directory integration configuration chosen.

14. If there were many conference room errors, try to determine the reason and fix it:

   a. Go to **Reports > Conference Room Errors** and verify that the time on the report is after the time when you received confirmation that the Active Directory is updated.

   b. Review the list of duplicate and invalid conference room IDs.

      Consider whether using a different Active Directory attribute, increasing the conference room ID length, or editing the characters to remove will resolve the majority of problems.

      If there are only a few problems, they can generally be resolved by correcting invalid Active Directory entries.

15. If necessary, repeat the previous steps, modifying the integration parameters as needed, until you get a satisfactory result.

**Related Links**

- [Microsoft Active Directory Integration](#)
- [Active Directory Cache Refresh Frequency](#)
- [Managing Users](#)
- [User Roles](#)

**Understanding Base DN**

The **Base DN** field is where you can specify the distinguished name (DN) of a subset of the Active Directory hierarchy (a domain, subset of domains, or organizational unit) to which you want to restrict the RealPresence DMA system.

It acts like a filter.

The following diagram illustrates how choosing different Base DN values affects which parts of a forest are included in the directory integration.
The Base DN field defaults to All Domains (which is equivalent to specifying an empty base DN in a query). Initially, the only other option is to enter a custom DN value. The first time you tell the system to connect to the Active Directory server, leave Base DN set to All Domains.

After the system has successfully connected to the Active Directory, the list contains entries for each domain in the Active Directory forest. If you want to restrict the system to a subset of the Active Directory (such as one tree of multiple trees, a subtree, a domain, or an organizational unit), select the corresponding base DN entry from the list.

### Adding Passcodes for Enterprise Users

You can add passcodes for enterprise users.

Polycom MCUs provide two optional security features for conferences, which the RealPresence DMA system fully supports:

**Use this Base DN:** To include the following:

- **All Domains**: 0–11
- **DC=nwind,DC=com**: 0–10
- **DC=nwind,DC=net**: 11
- **DC=eng,DC=nwind,DC=com**: 1–5
- **DC=mkt,DC=nwind,DC=com**: 6–8
- **DC=fin,DC=nwind,DC=com**: 9 & 10
- **DC=west,DC=eng,DC=nwind,DC=com**: 2
- **DC=east,DC=eng,DC=nwind,DC=com**: 3–5
- **OU=Planning,DC=fin,DC=nwind,DC=com**: 10
• **Conference Passcode** - A numeric passcode that callers must enter in order to join the conference.

• **Chairperson Passcode** - A numeric passcode that callers can enter to identify themselves as a conference chairperson. The chairpersons have additional privileges, like the ability to control recording. A conference can be configured to not start until a chairperson joins and to end when the last chairperson leaves.

**Note:** If Cisco Codian MCUs are included in the RealPresence DMA system's pool of conferencing resources, don't assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

If the RealPresence DMA system is integrated with your Active Directory, conference and chairperson passcodes for enterprise users can be maintained in the Active Directory.

You must determine which Active Directory attributes to use for the purpose and provide a process for provisioning users with those passcodes. If a user's passcode Active Directory attribute (either conference or chairperson) is left empty, the user's conferences won't require that passcode.

Passcodes must consist of numeric characters only (the digits 0-9). You can specify the maximum length for each passcode type (up to 16 digits). A user's conference and chairperson passcodes can't be the same.

When you generate passcodes for enterprise users, the RealPresence DMA system retrieves the values in the designated Active Directory attributes and removes any non-numeric characters from them. If the resulting numeric passcode is longer than the maximum for that passcode type, it strips the excess characters from the beginning of the string.

### Generate Chairperson and Conference Passcodes for Enterprise Users

You can generate chairperson and conference passcodes for enterprise users.

**Procedure**

1. In the Active Directory, select an unused attribute to be used for each of the passcodes.
   
   In a multi-domain forest, it's best to choose attributes that are replicated across the enterprise via the Global Catalog server mechanism. If the attributes you select are not available in the Global Catalog, the system can read them directly from each domain.

2. In the Active Directory, either provision users with passcodes or establish a mechanism for letting users create and maintain their own passcodes.
   
   Consult your Active Directory administrator for assistance with this.

3. On the RealPresence DMA system, go to **Integrations > Microsoft Active Directory**.

4. Complete the **Enterprise Chairperson and Conference Passcode Generation** section.
   
   a. Specify the Active Directory attribute from which to generate chairperson passcodes and the number of characters to use.

   b. Specify the Active Directory attribute from which to generate conference passcodes and the number of characters to use.

5. Click **Update**.

   After a short time, the system confirms that Active Directory configuration has been updated.
6. Note the time and click OK.
7. Confirm that passcode generation worked as expected.
   a. Go to Reports > Enterprise Passcode Errors and verify that the time on the report is after the time you got the confirmation that Active Directory configuration has been updated.
   b. Review the number of valid, invalid, and unassigned passcodes.
      If there are only a few problems, they can generally be resolved by correcting invalid Active Directory entries.

Active Directory Cache Refresh Frequency

Periodically, the system must refresh its cache of users, groups, and conference rooms from Active Directory.

As part of Active Directory integration, you can configure how often the system connects to Active Directory and updates its cache. Be aware that Active Directory cache refreshes can take a variable amount of time to complete, depending on the size of the directory and the amount of data being imported.

The initial import of data from Active Directory takes roughly three times as long as periodic refreshes. Active Directory cache refreshes may cause performance issues when the RealPresence DMA system is both under heavy call load and refreshing a large amount of data from the directory (potentially thousands of users). If a large number of users need to be imported from Active Directory and the RealPresence DMA system is subject to heavy call loads, you should schedule Active Directory cache refreshes during low-load hours.

Cache refresh times are scheduled for the timezone of the RealPresence DMA system where the refresh occurs, but are expressed in the timezone of the browser client. For example: You’re located in New York and schedule a cache refresh for 6:00am on a RealPresence DMA system located in London. The cache refresh occurs at 6:00am in the London time zone, but the Active Directory Integration dashboard pane shows the time of the most recent refresh as 2:00am, which was the local time (in New York) when the refresh occurred (in London).

Related Links
Integrate with Active Directory on page 201
Set Up Security
User Roles on page 443

Orphaned Groups and Users

When you manually update your Active Directory connection or when the system updates the connection automatically to refresh its cache, some Active Directory users and groups within the RealPresence DMA system may become orphaned.

Orphaned users and groups are no longer in the Active Directory or are no longer accessible to the RealPresence DMA system, but the system has local data for these orphaned users and groups (typically, local conference rooms or customized enterprise conference rooms).
Generate an Orphaned Groups and Users Report

You can generate an orphaned groups and users report to view orphaned users and groups that are no longer in the Active Directory or are no longer accessible to the RealPresence DMA system.

Procedure

» Go to Reports > MS Active Directory Reports > Orphaned Groups and Users.

The following table describes the fields included in the report.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group ID</td>
<td>ID of the user group.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the user group belonged.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>ID of the user.</td>
</tr>
<tr>
<td>First name</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the user belonged.</td>
</tr>
<tr>
<td>Roles</td>
<td>RealPresence DMA system user roles assigned to the user.</td>
</tr>
<tr>
<td>Conference rooms</td>
<td>RealPresence DMA system custom conference rooms assigned to the user.</td>
</tr>
</tbody>
</table>

Remove Orphaned Groups and Users

You can remove orphaned group data from the system.

Orphaned data is no longer usable by the system, so you can generally delete it. First, make sure that the system is successfully integrated to the correct Active Directory domain. Switching domains can cause many users and groups to be orphaned.

Procedure

1. Go to Reports > MS Active Directory Reports > Orphaned Groups and Users.
2. In the Actions list, click Clean Orphaned Groups.
3. When prompted to confirm, click OK.

The system removes the orphaned group data.
About the System's Directory Queries

The RealPresence DMA system uses the following subtree scope LDAP queries.

In a standard Active Directory configuration, all these queries use indexes.

The system runs the first three queries every time it creates or updates its cache as follows:

- When you click **Update** on the Microsoft Active Directory page.
- When the system restarts (if integrated with Active Directory).
- At the scheduled daily cache refresh time.

**User Search**

The user search queries the global catalog.

In a standard Active Directory configuration, all the filter attributes and attributes returned are replicated to the global catalog. The elements in italics are examples. The actual values of these variables depend on your configuration.

- **Base:** `<empty>`
  The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it's set to the default, All Domains, the base variable is empty, as shown. Otherwise, the base variable is the same as Base DN.

- **Filter:** `(&(objectCategory=person)(UserAccountControl: 1.2.840.113556.1.4.803:=512)(sAMAccountName=*)(!(userAccountControl: 1.2.840.113556.1.4.803:=2)))`
  The filter variable depends on the User LDAP filter setting.

- **Index used:** `idx_objectCategory:32561:N`
  The search used this index in our testing environment, using a standard Active Directory configuration (no indexes added). Results may be different for a different configuration, especially a different User LDAP filter setting.

- **Attributes returned:** `sAMAccountName, userAccountControl, givenName, sn, [ telephoneNumber ], [ chairpasscode ], [ confpasscode ]`
  The three attributes returned variables (in square brackets) are returned only if you specify the corresponding Active Directory attributes (for generating conference room IDs, chairperson passcodes, and conference passcodes, respectively) and if the attribute replication search determined that the attributes are replicated to the global catalog.

**Group Search**

The group search queries the global catalog.

In a standard Active Directory configuration, all the filter attributes and attributes returned are replicated to the global catalog.

- **Base:** `<empty>`
  The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it's set to the default, All Domains, the base variable is empty, as shown. Otherwise, the base variable is the same as Base DN.
Global Group Membership Search

The global group membership search queries LDAP.

- **Base:** DC=dma,DC=eng,DC=local
  
The base variable depends on the Base DN setting on the Microsoft Active Directory page. If it's set to the default, All Domains, the base variable is the domain DN, as shown by the example. Otherwise, the base variable is the same as Base DN.

- **Filter:** (&(objectClass=group)(groupType=-2147483646))

- **Indexes used:** idx_groupType:6664:N
  
The search used this index in our testing environment, using a standard Active Directory configuration (no indexes added). Results may be different for a different configuration.

- **Attributes returned:** member

Attribute Replication Search

The attribute replication search queries LDAP.

The system runs this query when it restarts (if already integrated with the Active Directory) and when you click the Update button on the Microsoft Active Directory page, but only if one or more of the configurable Active Directory attributes (for generating conference room IDs, chairperson passcodes, and conference passcodes) is specified.

The query determines if the Active Directory attributes are replicated to the global catalog. If they are, the user search retrieves them. If any of them are not, the system uses the configurable attribute domain search to retrieve the data from each domain controller.

- **Base:** CN=Schema,CN=Configuration, DC=dma,DC=eng,DC=local
  
The base variable depends on the forest root.

- **Filter:** (&(1LDAPDisplayName= telephoneNumber )(1LDAPDisplayName= chairpasscode )(1LDAPDisplayName= confpasscode ))

- **Indexes used:** idx_1LDAPDisplayName:3:N;idx_1LDAPDisplayName:2:N; idx_1LDAPDisplayName:1:N

  The search used these indexes in our testing environment, using a standard Active Directory configuration (no indexes added). Results may be different for a different configuration.

- **Attributes returned:** 1LDAPDisplayName, isMemberOfPartialAttributeSet
Configurable Attribute Domain Search

The configurable attribute domain search queries LDAP.

The system runs this query only if the attribute replication search determined that one or more of the configurable Active Directory attributes that it needs to retrieve (for generating conference room IDs, chairperson passcodes, and conference passcodes) isn't in the global catalog. In that case, it uses this query to retrieve the data from each domain controller.

- **Base:** DC=dma,DC=eng,DC=local
  The base variable depends on the domain name being queried.
- **Filter:** same as in the **User Search**
- **Index used:** same as in the **User Search**
- **Attributes returned:** sAMAccountName, attribute(s) not in global catalog

Domain Search

The domain search queries LDAP.

The system runs this query only when it restarts (if already integrated with the Active Directory) and when you click the **Update** button on the **Microsoft Active Directory** page.

- **Base:** CN=Configuration, ,DC=dma,DC=eng,DC=local
  The base variable depends on the forest root DN (the distinguished name of the Active Directory forest root domain).
- **Filter:** (&(objectCategory=crossRef)(systemFlags=3))
- **Indexes used:** idx_objectCategory:11:N
  The search used these indexes in our testing environment, using a standard Active Directory configuration (no indexes added). Results may be different for a different configuration.
- **Attributes returned:** cn, dnsRoot, nCName

Service Account Search

The service account search queries the global catalog.

In a standard Active Directory configuration, all the filter attributes and attributes returned are replicated to the global catalog.

The system runs this query only when you click the **Update** button on the **Microsoft Active Directory** page. It validates the service account ID.

- **Base:** <empty>
  The base variable depends on the **Base DN** setting on the **Microsoft Active Directory** page. If it's set to the default, **All Domains**, the base variable is empty, as shown. Otherwise, the base variable is the same as **Base DN**.
- **Filter:** (&(objectCategory=person)(UserAccountControl:1.2.840.113556.1.4.803:=512)(sAMAccountName=*)(& (!((userAccountControl:1.2.840.113556.1.4.803:=2)) (sAMAccountName= <userID> )))
  The first filter variable depends on the **User LDAP filter** setting. The second variable depends on the value entered in the **Service account ID** field on the **Microsoft Active Directory** page.
- **Index used:** idx_objectCategory:32561:N
The search used this index in our testing environment, using a standard Active Directory configuration (no indexes added). Results may be different for a different configuration, especially a different User LDAP filter setting.

- Attributes returned: sAMAccountName, userAccountControl, givenName, sn

**View the Active Directory Page**

You can view the Microsoft Active Directory page for reference.

**Procedure**

» Go to Integrations > Microsoft Active Directory.

The following table describes the fields on the Microsoft Active Directory page.

<table>
<thead>
<tr>
<th>Microsoft Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Integrate with enterprise directory server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Cluster</td>
</tr>
</tbody>
</table>
| Integration status | Integrated indicates that the server successfully connected to the Active Directory. If it didn’t, an error message appears.  
If you are an administrator, this label is a link to the Active Directory Integration Report. |
| User and group cache | Shows the state of the server’s cache of directory data and when it was last updated.                                                         |
| Refresh duration (seconds) | The duration of the processing of the most recent cache refresh.                                                                                 |
| Total users/rooms | Number of enterprise users and enterprise conference rooms in the cache. The difference between the two, if any, is the number of conference room errors.  
**Note**: If you don’t specify an Active Directory attribute for conference room ID generation, the number of rooms is zero. |
| Conference room errors | Number of enterprise users for whom conference rooms could not be generated.  
**Note**: If you don’t specify an Active Directory attribute for conference room ID generation, the number of errors equals the number of users. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orphaned groups and users</td>
<td>Number of orphaned users and groups (that is, users and groups that are disabled or no longer in the directory, but for whom the system contains data).</td>
</tr>
<tr>
<td></td>
<td>If you are an administrator, this label is a link to the Orphaned Groups and Users Report.</td>
</tr>
<tr>
<td>Enterprise passcode errors</td>
<td>Number of enterprise users for whom passcodes were generated that are not valid.</td>
</tr>
</tbody>
</table>

**General Integration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise directory server DNS name</td>
<td>If selected, the system uses serverless bind to find the closest global catalog servers. Enter the DNS domain name. We strongly recommend using this option.</td>
</tr>
<tr>
<td></td>
<td>If the system can’t determine the site to which it belongs, it tries to connect to any global catalog server.</td>
</tr>
<tr>
<td></td>
<td>If that fails, it uses the entered DNS domain name as a host name and continues as if the <em>IP address or host name</em> option were selected.</td>
</tr>
<tr>
<td></td>
<td>If this option is checked, the system attempts to connect to the Active Directory as follows:</td>
</tr>
<tr>
<td></td>
<td>1 It looks up the LDAP servers for the DNS domain (using DNS SRV: _ldap._tcp.&lt;domain-name&gt;).</td>
</tr>
<tr>
<td></td>
<td>2 It LDAP-pings every returned LDAP server until one responds with the system’s client site name.</td>
</tr>
<tr>
<td></td>
<td>3 It looks up the global catalog servers for the site (using DNS SRV: _gc._tcp.&lt;site-name&gt;._sites.&lt;domain-name&gt;).</td>
</tr>
<tr>
<td></td>
<td>4 It tries to connect to the global catalog servers.</td>
</tr>
<tr>
<td></td>
<td>5 If it can’t connect, it tries other global catalog servers from the forest.</td>
</tr>
<tr>
<td></td>
<td>6 If it still can’t connect, it uses the DNS domain name (using DNS A: &lt;domain-name&gt;) and connects to it.</td>
</tr>
<tr>
<td></td>
<td>Step 6 is the system behavior if this option is not checked.</td>
</tr>
<tr>
<td></td>
<td>The system’s network settings must have at least one domain name server specified.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP address or FQDN</td>
<td>If selected, the system attempts to connect to the Microsoft Active Directory domain controller specified. For a single-domain forest, enter the host name or IP address of a domain controller. For a multi-domain forest, Polycom doesn’t recommend using this option. If you must, enter the host name or IP address of a specific global catalog server, not the DNS domain name. The RealPresence DMA system can only integrate with one forest. A special Exchange forest (in which all users are disabled) won’t work because the system doesn’t support conferencing for disabled users.</td>
</tr>
<tr>
<td>Domain</td>
<td>The Active Directory domain in which the RealPresence DMA system should create and publish Active Directory contacts. If the system is upgraded from a version prior to 6.2 to version 6.2 or later, the initial value of this field is the Destination network of the SIP Peer configured in Skype pool to create/publish to in Conference Settings.</td>
</tr>
<tr>
<td>Domain\Enterprise Directory User ID</td>
<td>LDAP service account user ID for system access to the Active Directory. This must be set up in the Active Directory, but shouldn’t have Windows login privileges. Note: If you use Active Directory attributes that are not replicated across the enterprise via the Global Catalog server mechanism, the system must query each domain for the data. Make sure that this service account can connect to all the LDAP servers in each domain. The RealPresence DMA system initially assigns the administrator user role to this user, so you can use this account to give administrative access to other enterprise user accounts. Caution: Leaving a user role assigned to this account represents a serious security risk. For best security, remove the Administrator user role and mark this account disabled in the RealPresence DMA system (not the Active Directory) so that it cannot be used for conferencing or for logging into the RealPresence DMA system management interface.</td>
</tr>
<tr>
<td>Enterprise Directory User Password</td>
<td>Login password for service account user ID.</td>
</tr>
<tr>
<td>Security level</td>
<td></td>
</tr>
<tr>
<td>User LDAP filter</td>
<td>Specifies which user accounts to include (an underlying, non-editable filter excludes all non-user objects in the directory). The default expression includes all users that don’t have a status of disabled in the directory. Don’t edit this expression unless you understand LDAP filter syntax. See RFC 2254 for syntax information.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Base DN</td>
<td>Can be used to restrict the RealPresence DMA system to work with a subset of the Active Directory (such as one tree of multiple trees, a subtree, or a domain). Leave the default setting of All Domains.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cache Refresh</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Number of cache refreshes per day</td>
<td>The number of times per day that the RealPresence DMA system should log in to the directory server(s) and update its cache of user and group data.</td>
</tr>
<tr>
<td>Time of day to refresh cache</td>
<td>The time at which the RealPresence DMA system should log into the directory servers and update its cache of user and group data.</td>
</tr>
<tr>
<td></td>
<td>If the cache is refreshed more than once per day, this will be one of those times (but not necessarily the first time).</td>
</tr>
<tr>
<td>Territory for cache refresh</td>
<td>Specifies the territory whose RealPresence DMA system cluster is responsible for updating the user and group data cache.</td>
</tr>
<tr>
<td></td>
<td>In a superclustered system, this information is shared across the supercluster. The other clusters access the directory only to authenticate passwords.</td>
</tr>
<tr>
<td><strong>Enterprise Conference Room ID Generation</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Directory attribute</td>
<td>The name of the Active Directory attribute from which the RealPresence DMA system should derive conference room IDs (virtual meeting room numbers). Generally, organizations use a phone number field for this.</td>
</tr>
<tr>
<td></td>
<td>The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. If the attribute isn't in the Global Catalog, the system queries each domain controller for the data.</td>
</tr>
<tr>
<td></td>
<td>Leave this field blank if you don’t want the system to create conference rooms for the enterprise users.</td>
</tr>
</tbody>
</table>
### Characters to remove

The characters to be stripped from a phone number field's value to ensure a numeric conference room ID.

The default string includes \b, which represents the tab character. Use `\` to remove backslash characters.

If generating alphanumeric conference room IDs, remove the following: ()&%#@|":;,

Single spaces in the source field are preserved, but multiple consecutive spaces are concatenated to one space.

### Maximum characters used

The max length of conference room IDs.

The RealPresence DMA system strips excess characters from the beginning of the string, not the end. If you specify 7, the room IDs will contain the last 7 valid characters from the Active Directory attribute being used.

### Enterprise Chairperson and Conference Passcode Generation

#### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson directory attribute</td>
<td>The name of the Active Directory attribute that contains the chairperson passcodes. When choosing an attribute, remember that passcodes must be numeric. The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise using the Global Catalog server mechanism. If the attribute is not in the Global Catalog, the system queries each domain controller for the data. Leave this field blank if you don't want the system to create chairperson passcodes for the enterprise users.</td>
</tr>
<tr>
<td>Maximum characters used</td>
<td>Desired length of chairperson passcodes. The RealPresence DMA system strips excess characters from the beginning of the string, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.</td>
</tr>
<tr>
<td>Conference directory attribute</td>
<td>The name of the Active Directory attribute that contains the conference passcodes. In choosing an attribute, remember that passcodes must be numeric. The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. But if the attribute is not in the Global Catalog, the system queries each domain controller for the data. Leave this field blank if you don't want the system to create conference passcodes for the enterprise users.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum characters used</td>
<td>Desired length of conference passcodes. The RealPresence DMA system strips excess characters from the beginning of the string, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.</td>
</tr>
</tbody>
</table>
Skype RealConnect

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Callback contacts OU | The OU the system should use for managing Active Directory contacts used for callbacks. The feature of hosting RealConnect conferences on external Skype systems requires Active Directory contact names to be passed with the signaling between the external Skype system and the Polycom MCU. These contact names enable the external Skype system to call back to the Polycom MCU. The RealPresence DMA system manages a pool of these contacts, which can be used for this purpose. The system uses all of the contacts that it finds in the specified OU as part of this pool. When the system starts a new conference through the dial rule action **Resolve to Skype Conference ID by Conference Auto Attendant**, it selects an unused contact from the pool and provides the contact name to the Polycom MCU for use in its signaling. Once the conference has ended, the RealPresence DMA system reclaims the contact for reuse. For example: If you create a container for callback contact accounts at the root of your Active Directory domain called CallbackContacts, specify:

```bash
ou=CallbackContacts
```

for this field. If `CallbackContacts` is under the Development container, specify:

```bash
ou=CallbackContacts,ou=Development
```

for this field. For more information on how to configure callback contact accounts in Active Directory, see the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide*. **Note:** Within the Active Directory, all of the callback contacts must exist within the specified OU, and you must enable the setting **Enable for Skype Server** for each contact. You must also ensure that there are enough callback contacts in the OU for the cluster to use under heavy conferencing loads. There can be up to 2400 concurrent RealConnect conferences hosted on external Skype systems.

**Related Links**

- [User Roles](#) on page 443
Microsoft Exchange Server Integration

Topics:

- Polycom Solution and Integration Support
- Differences Between Calendaring and Scheduling
- Microsoft Exchange Server Page
- Exchange Server Integration

To support Polycom Conferencing for Microsoft Outlook, you can integrate the RealPresence DMA system with your Microsoft Exchange server.

This integration enables users who install the Polycom conferencing Add-in for Microsoft Outlook to set up Polycom conferencing meetings in Outlook.

When you integrate the RealPresence DMA system with an Exchange server, it connects to the Exchange server as the Polycom conferencing user and subscribes to notifications. The Exchange server notifies the RealPresence DMA system as soon as a meeting invitation (or other mail) arrives in the Polycom conferencing user inbox. It also sends heartbeat messages to verify that the subscription is working.

If the RealPresence DMA system fails to receive a heartbeat or other notification for 30 seconds, it begins checking its inbox every 4 minutes for new messages, and also attempts to reestablish the subscription (push connection) each time.

As with other Outlook meeting requests, the meeting organizer invites attendees and specifies where and when to meet. The where in this case is a conference room, or VMR, on the RealPresence DMA system.

The invitees may include conference-room-based Polycom HDX systems as well as users with Polycom HDX personal conferencing endpoints. Polycom HDX systems monitor an Exchange mailbox (either their own or a linked user's) for Polycom conferencing meeting invitations.

Invitees with a desktop conferencing client (such as Polycom RealPresence Desktop) can join the meeting by clicking a link in the Outlook reminder or calendar. Invitees with a Polycom HDX endpoint can join by clicking a link on the HDX system's reminder.

The add-in also sends Polycom conferencing meeting invitations to a Polycom conferencing user mailbox on the Exchange server. The RealPresence DMA system accepts or declines these invitations. A meeting invitation is declined if:

- The VMR number is in use by any other conference room (calendared, enterprise, or custom).
- The user sending the invitation is not in the RealPresence DMA system's Active Directory cache.
- The invitation contains invalid or incomplete meeting data.
- The meeting's duration exceeds the system's **Default Conference Duration** setting.
- The conference or chairperson passcode is not valid.
Polycom Solution and Integration Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only.

Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services, and its certified Partners, to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments. Polycom Collaboration Services for Microsoft integration are mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server integrations. See http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative for more information.

Differences Between Calendaring and Scheduling

Calendaring isn’t the same as scheduling.

Using the Polycom conferencing Add-in for Microsoft Outlook to set up a meeting appointment doesn’t reserve video resources, and invitations are not declined due to lack of resources.

The RealPresence DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as part of its conferencing resource pool. If you use Codian MCUs to host Polycom conferencing (calendared) meetings, be aware of these limitations:

- Codian MCUs don’t support the Polycom conferencing Add-in’s recording and streaming options.
- Codian MCUs don’t provide the gathering phase that RMX and RealPresence Collaboration Server MCUs provide at the beginning of the conference.

Codian MCUs can’t receive and accept Outlook meeting invitations themselves, and can only be used if a RealPresence DMA system is part of the Polycom conferencing for Outlook solution.

Microsoft Exchange Server Page

The following table describes the fields on the Microsoft Exchange Server page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable integration with Microsoft Exchange Server</td>
<td>Enables the Exchange server integration fields and the Update button, which initiates a connection to the Microsoft Exchange server.</td>
</tr>
<tr>
<td>Exchange Server address</td>
<td>FQDN or IP address of the Exchange server.</td>
</tr>
<tr>
<td>Domain/user name</td>
<td>The user ID for the Polycom conferencing infrastructure mailbox on the Exchange server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the Polycom conferencing user ID.</td>
</tr>
<tr>
<td>Territory</td>
<td>Select a territory, thereby determining which RealPresence DMA cluster is responsible for integrating with the Exchange server and monitoring the Polycom conferencing infrastructure mailbox.</td>
</tr>
</tbody>
</table>
### Exchange Server Integration

Unless the **Allow unencrypted calendar notifications from Exchange server** option is enabled in **Security Settings**, the RealPresence DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface.

The Exchange server must be configured to trust the certificate authority in order for the RealPresence DMA system to subscribe to notifications.

If the RealPresence DMA system is configured with a self-signed certificate and the **Allow unencrypted calendar notifications from Exchange server** security option is disabled, Exchange server integration will fail.

If the RealPresence DMA system is unable to subscribe to notifications, the Exchange Server status (see Dashboard) displays **Subscription pending** indefinitely and the RealPresence DMA system doesn’t automatically receive calendar notifications. Instead, it must check the Polycom conferencing mailbox for meeting request messages, which it does every 4 minutes.

### Integrate the Polycom RealPresence DMA System with Your Exchange Server

To enable Polycom Conferencing for Microsoft Outlook, you need to integrate the RealPresence DMA system with your Exchange server.

Before integrating with your Exchange server, ensure that the RealPresence DMA system is integrated with Microsoft Active Directory.

**Procedure**

1. Confirm that the RealPresence DMA system has been successfully integrated with your Active Directory and verify the domain.
2. Ensure that the DNS server used by the Microsoft Exchange server (usually, the nearest Active Directory domain controller) has an A record for the RealPresence DMA system that resolves the system’s FQDN to its virtual IP address.
3. On the Microsoft Exchange server, create the Polycom Conferencing user that the add-in will automatically invite to Polycom Conferencing meetings.
   a. For the user ID, specify the same domain used to integrate with the Active Directory.
   b. Enter the Display Name as you want it to appear in the **To** field of invitations.
      For example, Polycom Conference (first and last name).
4. Go to **Integrations > Microsoft Exchange Server**.
5. Select **Enable integration with Microsoft Exchange Server** and specify the address (host name or IP address) of the Exchange server.
6. Specify the login credentials for the system on the Exchange server.
7. Set **Territory** to the territory of the Polycom RealPresence DMA cluster responsible for calendaring.

8. If you have multiple Exchange servers behind a load balancer, add each individual Exchange Server's IP address under **Accept Exchange notifications from these additional IP addresses**.

9. Click **Update**.
   
   A dialog informs you that the configuration has been updated.

10. Click **OK**.

11. Install the Polycom Conferencing Add-in for Microsoft Outlook on your PC and create the configuration you want distributed to your users.
   
   Optionally, customize the invitation template(s).

12. Distribute the Polycom Conferencing Add-in for Microsoft Outlook, its configuration file, and customized templates to your users (see the *System Administrator Guide for the Polycom Conferencing Add-in for Microsoft Outlook*).
Microsoft Skype for Business Integration

Topics:

- Lync 2013 vs. Skype for Business 2015 Integration
- Scheduled Conferences with Polycom RealConnect
- Automatic Contact Creation and Configuration
- Active Directory Service Account Permissions
- Skype and non-Skype Endpoint Collaboration
- Considerations and Requirements for Integration with Skype for Business 2015
- Lync 2010 and 2013 Client / Server Feature Support
- Integrate RealPresence DMA and Skype for Business 2015
- Diagnose Presence Problems


When you integrate the RealPresence DMA system into a Skype for Business environment, the system communicates with the Skype servers and Active Directory to provide contact presence and conference interaction between MCUs managed by the RealPresence DMA system and the Skype for Business AVMCU. Presence allows Skype clients to view the presence of a RealPresence DMA system VMR, similar to any other contact in the Skype client contact list.

The RealPresence DMA system can be integrated with Lync 2013 if you haven't yet upgraded your environment to Skype for Business.

Note: Throughout this guide, the term Polycom conference contact represents an Active Directory contact that corresponds with a VMR on the RealPresence DMA system and allows Skype presence status to be published for that VMR. You can configure the RealPresence DMA system to create and delete Polycom conference contacts automatically.

Callers can also connect to a conference containing a mixture of Skype clients and other endpoints.

The following topics describe integration with Skype for Business:

Lync 2013 vs. Skype for Business 2015 Integration

The RealPresence DMA system can interact with both Lync 2013 and Skype for Business 2015 environments.

However, there are some differences between interacting with a Lync 2013 environment and full integration with a Skype for Business 2015 environment.
When the RealPresence DMA system is integrated with Lync 2013, Lync clients that connect to RealPresence DMA system VMRs may be hosted on the Lync AVMCU, and can be part of RealPresence DMA system conferences via a cascade link that the Polycom MCU creates with the AVMCU.

Integration also allows a non-Lync client to connect to a Lync 2013 scheduled conference by dialing the Lync conference ID included in the Microsoft Outlook meeting invitation. The RealPresence DMA system receives the connection attempt, creates a matching VMR automatically, and builds a cascade link between a Polycom MCU and the Lync AVMCU.

When the RealPresence DMA system is integrated with Skype for Business 2015, conferencing connections for Skype and non-Skype clients function as described for Lync 2013. However, Polycom RealConnect conferences with Lync 2013 and Skype for Business 2015 Server (on premise) also benefit from Skype MCU affinity.

Skype for Business deployments can be geographically distributed. When you use Polycom RealConnect technology, video conferences can occur on various Skype AVMCUs deployed throughout the geography. Skype MCU affinity enables the RealPresence DMA system to select a Polycom MCU in proximity to the Skype AVMCU hosting the Polycom RealConnect conference. This capability can reduce call latency, traffic, and costs.

### Scheduled Conferences with Polycom RealConnect

The Polycom RealConnect scheduled conference scenario is a single workflow for scheduling conferences for Skype and non-Skype endpoints.

Once you integrate your system with a Skype for Business 2015 environment, registered endpoints can call through the RealPresence DMA system and join conferences that you schedule with Microsoft Outlook. The Polycom conferencing for Outlook (PCO) plug-in isn’t needed for Polycom RealConnect.

**Note:** Polycom RealConnect scheduled conferences require that the RealPresence DMA system manage at least one Polycom MCU that supports Skype for Business 2015. Non-Polycom MCUs are not supported.

Polycom RealConnect uses Microsoft Outlook meeting invitations to deliver conference information to participants. When you schedule a conference with Outlook, you can configure the Outlook meeting invitation to include Skype conference IDs as plain text, in addition to the automatically included Join Skype Meeting hypertext link. When they receive the meeting invitation, users of Skype clients can click the link, and users of non-Skype endpoints can dial the plain-text Skype conference ID.

When non-Skype endpoints dial the meeting ID in the meeting invitation, the RealPresence DMA system responds to the incoming call by applying a dial rule with the action Resolve to Skype conference ID. This dial rule prompts the RealPresence DMA system to search any of the dial rule’s configured and selected SIP peers (representing Skype front-end pools) for a matching Skype conference. If the meeting ID isn’t resolved on one of the selected SIP peers, the system continues to attempt to resolve the dial string using the next dial rule in the list.

If the conference ID is resolved on one of the selected SIP peers, the SIP peer gives the RealPresence DMA system the focus URI of the conference. From this information, the RealPresence DMA system extracts Skype user information, then queries the Skype for Business deployment to obtain the FQDN of the front-end pool, which hosts the AVMCU conference. Once the RealPresence DMA system receives a response, it searches the selected SIP peers in the dial rule for a next hop address that matches the front-end pool FQDN. When the system finds a match, it uses the MCU pool order configured in the matching external SIP peer to select the MCU to host the conference. The RealPresence DMA system
dynamically creates a VMR and, using the configured MCU pool order, starts a conference on a Polycom MCU in proximity to the Skype AVMCU that is hosting the Polycom RealConnect conference. Using the Skype focus URI received from the RealPresence DMA system, the MCU builds a cascade link between the newly created conference and the Skype AVMCU. Skype clients and non-Skype endpoints can now interact in the conference. If there’s no selected SIP peer with a matching FQDN, or if the matching SIP peer doesn’t have a configured MCU pool order, the RealPresence DMA system uses the MCU pool order configured in the dial rule.

In a superclustered configuration, endpoints can connect to a Polycom RealConnect conference from any cluster in the supercluster, but the call will be routed through the supercluster to the cluster that is hosting the Polycom RealConnect conference.

If the RealPresence DMA system loses connection with a Skype server, the system tries to reconnect and alerts the administrator of the outage.

For information on configuring Microsoft Outlook and Microsoft RealPresence DMA to support Polycom RealConnect, refer to the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide.

**Automatic Contact Creation and Configuration**

You can configure the RealPresence DMA system to create and manage a corresponding Polycom conference contact in Active Directory whenever users create a new VMR.

The RealPresence DMA system communicates with the Skype server to ensure that the new contact is enabled for Skype functionality. This allows the system to publish presence updates to the conference contact; Skype clients display a status of **Available**, **Busy**, or **Offline** for the conference contact in the client's contact list.

---

**Note:** When you manually or automatically create a VMR or group of VMRs, allow up to 10 minutes for the newly created conference contact(s) to appear in the Skype client contact list.

---

**Active Directory Service Account Permissions**

If you integrate the RealPresence DMA system with Skype for Business 2015 and plan to use the automatic conference contact creation feature, note that the required Active Directory service account should have full permissions to add, change, and delete entries in the OU where the conference contacts are stored.

The account should also have full administrative permissions for Skype administration to manipulate these contacts.

**Skype and non-Skype Endpoint Collaboration**

Callers with Skype clients and non-Skype endpoints can join the same conference in several ways.

See the Microsoft Skype for Business documentation for more details on specific call flows.

- Users of Skype clients can select a Polycom conference contact in the contact list and drag it to an ongoing Skype conversation window, starting a video call.
Users of Skype clients can start a Skype conference by selecting the **Show Menu** icon and choosing **Meet Now**. After starting the conference, users can invite more attendees to the conference or drag a Polycom conference contact into the conversation window to add the participant.

Users of Skype clients can right-click a Polycom conference contact in the contact list and choose **Start a video call**.

Users of Skype clients and other endpoints can use a Microsoft Outlook meeting invitation to connect to a Skype conference. Non-Skype endpoints can dial the included conference ID, and Skype clients can click the **Join Skype Meeting** link included in the invitation.

When you register a Polycom endpoint to a RealPresence DMA system and make a point-to-point call to a Lync 2013 or Skype for Business 2015 client, the conference may not have video because the H.261 and H.263 video codecs are not supported by the Lync or Skype client. As a workaround for Polycom HDX and RealPresence Group Series endpoints, register the endpoint to the Lync or Skype server before starting the conference. This workaround requires an RTV option key or Lync/Skype Interoperability License.

### Considerations and Requirements for Integration with Skype for Business 2015

- For the latest software version requirements and interoperability information, consult the *Polycom Unified Communications in a Microsoft Environment Release Notes*.

- The following Virtual Entry Queue (VEQ) call scenarios are not supported:
  - Calls to a Virtual Entry Queue (VEQ) from a Skype client
  - A non-Skype endpoint connecting to a VEQ and entering a Skype conference ID when prompted

- **Conference mode** configurations of **SVC-only** and **Mixed AVC and SVC** are not supported in RealPresence DMA system and Skype cascaded conferences. Any conference that requires Skype AVMCU connectivity must use conference templates with **AVC only** as the configured **Conference mode**.

- You need Skype-capable Polycom MCUs to use Polycom RealConnect functionality. Non-Polycom MCUs are not supported. If your Polycom MCU is Skype-capable, the Skype icon displays next to the MCU name on the **Integrations > MCU** page. If no MCUs that support Skype for Business are available, the cascaded Polycom RealConnect conference won't start. Refer to your MCU documentation for more information.

- The **Transfer Call** feature of the Lync or Skype client isn't supported when the MCU hosting the call is configured to use ICE or encryption.
# Lync 2010 and 2013 Client / Server Feature Support

The following table outlines features that the RealPresence DMA system supports in Lync 2010 and Lync 2013 client and server environments.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Client</th>
<th>Server</th>
<th>Uses SVC cascading between Microsoft AVMCU and Polycom MCU</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling - Dial to RealConnect conference</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-point Lync conferences invite a VMR</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meet Now calls to a VMR</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escalated conferences - Lync client drag-and-drop multi-party call</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct point-to-point Lync call to a VMR</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Skype 2015</td>
<td>Skype 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMA registered endpoint calling point-to-point to a Lync client</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td>If a Lync 2013 client, all calls will be audio only.*</td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lync client calling point-to-point to DMA registered endpoint</td>
<td>Lync 2010</td>
<td>Lync 2010</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence enabled VMRs</td>
<td>Lync 2013</td>
<td>Lync 2013</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

* The Lync 2010 client supports the H.263 video codec, but the Lync 2013 client doesn't.
Integrate RealPresence DMA and Skype for Business 2015

Refer to the *Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide* for the tasks needed to integrate the RealPresence DMA system with Skype for Business 2015.

If you need the RealPresence DMA system to automatically create conference contacts in Active Directory, ensure that your system is integrated with Microsoft Active Directory before proceeding.

Diagnose Presence Problems

If after integration your Skype client doesn’t display presence for RealPresence DMA system VMRs when you enable automatic contact creation and presence publishing, use the following points to begin troubleshooting.

- Check for any active system alerts
  
  The description of any active system alerts can indicate potential issues with integration. See the online help or the *Polycom RealPresence DMA System Operations Guide* for a description of the alert text.

- Verify NTP Lync server and RealPresence DMA system use the same NTP source
  
  If the system time differs slightly between the RealPresence DMA system and the Skype server, the Skype server can reject contact creation attempts. See the Admin > Server > Time Settings page to configure NTP servers.

- Ensure supported MCUs are in service with available ports
  
  See the Integrations > MCU page for an overview of MCU status.

- Ensure that the Publish presence for Polycom conference contacts check box is enabled
  
  This setting, on the Service Config > Conference Manager Settings > Conference Settings page, controls system-wide presence publishing for conference contacts.
RealPresence Resource Manager Integration

Topics:

- Considerations When Integrating with a RealPresence Resource Manager System

Integrating with a RealPresence Resource Manager system provides the RealPresence DMA system with the following information:

- All site topology information configured in the RealPresence Resource Manager system.
  
  The RealPresence DMA system uses site topology information for a variety of purposes, including cascade for bandwidth conferences, bandwidth management, and Session Border Controller selection.

- All user-to-device associations configured in the RealPresence Resource Manager system in which the enterprise user is also known to the RealPresence DMA system.
  
  The RealPresence DMA system uses user-to-device associations to assign classes of service to endpoints based on the user they belong to.

**Note:** The RealPresence DMA system currently does not support integration with a RealPresence Resource Manager system when the RealPresence DMA system is configured for split network interfaces.

Integrating with a RealPresence Resource Manager system allows you to configure site topology and user-to-device associations in one place instead of two, ensuring consistency. While integrated, you can only configure this information in the RealPresence Resource Manager system. If you do not have a RealPresence Resource Manager system, or if the RealPresence DMA system and RealPresence Resource Manager system are not integrated, both site topology and user-to-device associations can be manually configured in the RealPresence DMA system. If the integration is terminated, the RealPresence DMA system retains the information last received from the RealPresence Resource Manager system. You can then edit this information in the RealPresence DMA system.

When the RealPresence DMA system gets its site topology information from a RealPresence Resource Manager system, the first three territories assigned to a RealPresence DMA cluster are enabled for conference rooms.

The **Bit rate to bandwidth conversion factor** setting on the Call Server Settings page of the RealPresence DMA system can affect choices for bandwidth restrictions in your site topology. Since the RealPresence Resource Manager system calculates call bandwidth requirements using a conversion factor of 2.5, Polycom recommends using a **Bit rate to bandwidth conversion factor** value of 2.5 if you integrate with a RealPresence Resource Manager system. Otherwise, you'll need to alter the bandwidth restrictions for your site topology to take the conversion factor value into account. This ensures that the RealPresence DMA system's call bandwidth requirement calculations are predictable.
Considerations When Integrating with a RealPresence Resource Manager System

When integrating a RealPresence Resource Manager system with a RealPresence DMA system, be aware of the following:

- The RealPresence DMA system requires the RealPresence Resource Manager system to have a Subject Alternative Name (SAN) in its certificate to use in the TLS handshake between the two systems. The default self-signed certificate doesn’t contain a SAN. The RealPresence Resource Manager administrator needs to regenerate a certificate with a SAN before integrating with the RealPresence DMA system if the system will be used to schedule pooled conferences and site topology is integrated.
- DNS servers must be able to resolve the RealPresence DMA system’s FQDN to its IP address and the RealPresence Resource Manager system's FQDN to its IP address.
- When you integrate a RealPresence Resource Manager system with a RealPresence DMA supercluster with embedded DNS enabled, in the RealPresence Resource Manager's Add DMA dialog, select Support DMA Supercluster.
- Integrating a RealPresence Resource Manager system with a RealPresence DMA system enables the RealPresence Resource Manager system to use the RealPresence DMA system’s API to set up and monitor scheduled and preset dial-out (anytime) conferences using the RealPresence DMA system's resources.
- If the Allow delegated authentication to enterprise directory server option on the RealPresence Resource Manager system isn’t configured or working properly, the RealPresence DMA system doesn’t receive user-to-device association data for enterprise users and intermittently generates Alert 2001.
- If you plan to configure two RealPresence DMA nodes as a HA pair, you must configure the network settings to enable the HA settings before you integrate with a RealPresence Resource Manager system.

Integrate with a RealPresence Resource Manager System

You can integrate the RealPresence DMA system with a RealPresence Resource Manager system from the Network Device > DMA page of the RealPresence Resource Manager management interface.

View RealPresence Resource Manager Integration Details

When your RealPresence DMA system is integrated with a RealPresence Resource Manager system, you can view the integration details from the RealPresence DMA system.

Procedure

» Go to Integrations > RealPresence Resource Manager.

The RealPresence Resource Manager Integration Details display. The following table describes the fields in the list:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Name of the system.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the system.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Version</td>
<td>Software version of the system.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of last attempt to contact system (OK or Unreachable).</td>
</tr>
<tr>
<td>Time</td>
<td>Time of last attempt to contact the system.</td>
</tr>
</tbody>
</table>

**Terminate RealPresence Resource Manager Integration**

When the RealPresence DMA system is integrated with a RealPresence Resource Manager system, the **RealPresence Resource Manager** page contains the **Leave RealPresence Resource Manager** command, which you can use to terminate the integration.

You can’t use this page to integrate with a RealPresence Resource Manager system.

**Procedure**

1. Go to **Integrations > RealPresence Resource Manager**.
2. Under **Actions**, select **Leave RealPresence Resource Manager**.
3. When asked to confirm that you want to leave, click **Yes**.
   
   The system connects to the RealPresence Resource Manager system, terminates the integration, and informs you when the process is complete.
4. On the **RealPresence Resource Manager** page, verify that the RealPresence DMA system is no longer integrated with the RealPresence Resource Manager system.

   If the integration is terminated, the RealPresence DMA system retains the site topology and user-to-device association information last received from the RealPresence Resource Manager system. You can then edit this information in the RealPresence DMA system.
Polycom ContentConnect Integration

Topics:

- Load Balancing Multiple Polycom ContentConnect Systems
- Geo-Affinity for Polycom ContentConnect Systems
- High Availability for Polycom ContentConnect Systems
- Using Embedded DNS to Share Polycom ContentConnect Systems Across a Supercluster or HA Pair

The Polycom RealPresence DMA system can provide load balancing for multiple Polycom ContentConnect systems.

In a Microsoft Skype for Business environment, a ContentConnect system provides gateway services when a Polycom conference is cascaded to a corresponding Skype for Business conference. To detect this cascade, a ContentConnect system uses the RealPresence DMA system's subscribe and notify service, which reports when a conference is started and when that conference is cascaded.

Each ContentConnect system has limited capacity for gateway services. A single ContentConnect server may not be able to scale to handle the entire load for deployments with large numbers of conferences. In this case, multiple ContentConnect systems can be pooled. Each system must use the subscribe and notify service, which doesn't filter notifications. Therefore, all ContentConnect systems will receive notifications for all conferences and all systems will attempt to join every cascaded conference.

The RealPresence DMA system load balancing feature filters notifications. Multiple ContentConnect systems can subscribe for conference information and the RealPresence DMA system will deliver only a subset of the active conferences to each individual ContentConnect system.

Note that load balancing doesn't occur for conferences that are already in progress.

Load Balancing Multiple Polycom ContentConnect Systems

A RealPresence DMA system can act as a load balancer for a pool of Polycom ContentConnect systems.

A pool of ContentConnect systems can also be shared across a supercluster or High Availability (HA) pair of RealPresence DMA systems by pointing each system in the pool to a RealPresence DMA system’s embedded DNS FQDN. See Using Embedded DNS to Share Polycom ContentConnect Systems Across a Supercluster or HA Pair in this guide.

To establish communication between a RealPresence DMA system and the ContentConnect systems, you need to complete the following steps:

1. Enable ContentConnect load balancing on the RealPresence DMA system.
2. Point multiple ContentConnect systems to the RealPresence DMA system's SIP server address and load balancing virtual server address.

After you complete the preceding steps, the ContentConnect systems will display in the RealPresence DMA system's list of Available ContentConnect systems.
For instructions on configuring ContentConnect systems to use the RealPresence DMA system as a load balancer, see the Polycom ContentConnect Administrator Guide, available on the Polycom support site (support.polycom.com).

Enable Load Balancing

From the RealPresence DMA system management interface, you can enable load balancing for multiple Polycom ContentConnect systems.

Once you enable the feature, the ContentConnect systems that point to the RealPresence DMA system will display in the list of Available ContentConnect systems. You can also disable load balancing when necessary.

Procedure

1. Go to Integrations > Polycom ContentConnect.
2. Select Load balance multiple ContentConnect systems to enable the RealPresence DMA system to function as a load balancer.
3. Click Update.
4. Click Yes to confirm.
5. Click Update to save the load balancing settings.

Add a Content Server Manually

If a Polycom ContentConnect system is configured to connect to the RealPresence DMA system, it's listed in Available ContentConnect systems.

If a ContentConnect system doesn’t display in the list, you can add it manually from your RealPresence DMA system.

Procedure

1. Go to Integrations > Polycom ContentConnect.
2. Click the Add button.
3. Complete the fields as described in the following table:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content server name</td>
<td>The name of the ContentConnect system to connect to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Content server address</td>
<td>The IP address of the ContentConnect system.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the ContentConnect system.</td>
</tr>
<tr>
<td>Enabled</td>
<td>When selected, load balancing is enabled for this ContentConnect system.</td>
</tr>
</tbody>
</table>

4. Click OK.

### Disable Load Balancing for a ContentConnect System

From the RealPresence DMA system management interface, you can disable load balancing for individual ContentConnect systems.

If you disable load balancing for a ContentConnect system, any active calls will continue until finished but no new calls will be routed to that system.

You can also enable load balancing for a ContentConnect system that you previously disabled.

**Procedure**

1. Go to **Integrations > Polycom ContentConnect**.
2. From the list of **Available ContentConnect systems**, select the system for which to disable load balancing.
3. Click the **Disable** button.
   
   The **Enabled** column in the **Available ContentConnect systems** list displays **false** for a disabled system.

### Geo-Affinity for Polycom ContentConnect Systems

The RealPresence DMA system provides geo-affinity for ContentConnect systems through MCU pool configuration.

You can add both MCUs and ContentConnect systems to an MCU pool, then add the pool to a pool order and assign it to a user conference room (VMR). When a call to the VMR lands on one of the MCUs in the pool, the RealPresence DMA system will also look for ContentConnect systems within the pool. If the pool has ContentConnect systems with available capacity, the RealPresence DMA system will load balance among them by routing calls to the ContentConnect system with the highest available capacity. If the pool does not contain any ContentConnect systems, or if none have capacity, the RealPresence DMA system will look within the pool order for an MCU that the call can land on. If the call successfully lands on an MCU, the system looks for available ContentConnect systems that are in the same pool as the MCU. If none are available, the RealPresence DMA system does not reselect an MCU but will look for any available ContentConnect system, regardless of its geographic location. The MCU selection is the highest priority.
High Availability for Polycom ContentConnect Systems

The RealPresence DMA system can provide integrated load balancing for Polycom ContentConnect systems that are configured for HA.

When a ContentConnect system that's a member of an HA pair subscribes to the RealPresence DMA system, the DMA system will automatically add an enabled record to its list of Available ContentConnect systems. The record identifies the ContentConnect system's physical IP address, not the virtual address of the HA cluster. Two records are needed for the HA pair of ContentConnect systems - each record identifies the physical IP address for one of the systems. However, the RealPresence DMA system will initially create only the record for the current master ContentConnect system. When the current master fails over to the current slave, the RealPresence DMA system will create a record for the new master.

Configure a Polycom ContentConnect HA Pair for Load Balancing

When you configure a ContentConnect HA pair for load balancing, you need to initiate a failover to get both ContentConnect system records into the RealPresence DMA system, or manually add the current slave's physical IP address as a ContentConnect system record in the RealPresence DMA system.

You then need to disable the two records and add a third record that points to the virtual IP address of the ContentConnect HA pair.

The end state should be three records for the HA pair - two disabled records pointing to physical IP addresses and one enabled record pointing to the virtual IP address.

Procedure

1. Go to Integrations > Polycom ContentConnect.
2. Complete one of the following actions:
   - Initiate a failover from the current master ContentConnect system to the current slave system.
     The RealPresence DMA system adds a record for the new master.
   - Manually add the current slave system's IP address as a ContentConnect system record in the RealPresence DMA system.
3. Disable the two ContentConnect HA system records.
4. Click the Add button to add a third record that points to the virtual IP address of the ContentConnect HA pair.
5. Click Update to save the settings.
Using Embedded DNS to Share Polycom ContentConnect Systems Across a Supercluster or HA Pair

A pool of Polycom ContentConnect systems can be shared across a supercluster or High Availability (HA) pair by pointing each system in the pool to a RealPresence DMA system's embedded DNS FQDN.

The ContentConnect systems will service the primary cluster if it's active. If the primary cluster goes out of service, the ContentConnect systems will redirect to the backup cluster until the primary cluster becomes active again.

The embedded DNS configuration enables full use of all ContentConnect systems and prevents the need to point an individual ContentConnect system to each RealPresence DMA system in the supercluster.

Configure the RealPresence DMA Embedded DNS FQDN in a Polycom ContentConnect System

If you have a supercluster with a primary and backup RealPresence DMA system configured in a territory, you can specify the embedded DNS FQDN of the RealPresence DMA system.

If the primary system fails over, the backup system will continue to use the same pool of ContentConnect devices for future conferences until the primary RealPresence DMA system is back online.

Procedure

1. From the ContentConnect system's user interface, go to Server Configuration > Server.
2. In the SIP Server Address field, enter the RealPresence DMA system's embedded DNS FQDN.
3. Restart the ContentConnect system.
4. From the RealPresence DMA system's user interface, go to Integrations > Polycom ContentConnect.

   The Available ContentConnect systems list displays all ContentConnect systems connected to the RealPresence DMA system.
VPN Tunnel Settings

Topics:

- Add a VPN Tunnel
- Run the RealPresence DMA Edge Wizard on both VPN Tunnel Systems
- Enable Endpoint Provisioning through a VPN Tunnel

The RealPresence DMA system supports VPN tunneling to other RealPresence DMA systems through the use of OpenVPN.

Once you configure a VPN tunnel, all communication goes through the tunnel. If the tunnel goes down, no communication can occur until you disable or delete the VPN tunnel on both edge-configured RealPresence DMA systems. When the tunnel is disabled or deleted, communication can resume via the typical channels.

Use of a VPN tunnel will decrease overall call capacity from approximately 1000 concurrent calls to approximately 500 concurrent calls, depending on call settings and use.

Note that when you create a VPN tunnel between your RealPresence DMA edge systems, you need to set up access proxy settings that enable the VPN tunnel to support provisioning.

Related Links
Enable Endpoint Provisioning through a VPN Tunnel on page 242

Add a VPN Tunnel

You can configure a VPN tunnel between an edge-configured system in the corporate DMZ or external to the corporate firewall and a second edge-configured system inside your enterprise network.

You can configure the VPN Tunnel Settings on either system first, then use the Configure Remote DMA option to automatically set up the second system. If automatic configuration isn’t an option due to firewall restrictions on REST API commands, you can manually configure the remote system.

When you configure the VPN tunnel settings, the local system refers to the system you're currently configuring. The remote system is the other end of the tunnel, regardless of location (inside or outside your enterprise network).

Note: You must be logged in to the management user interface on both RealPresence DMA edge-configured systems when you create a VPN tunnel.

If you have more than one network interface (for example, signaling and media), you need to set up multiple VPN tunnels, with one tunnel for each service on each different network interface between the two edge systems. The private IP address on the outside edge system must point to the public IP address on the inside edge system. Configure like-to-like network interfaces, that is, signaling-to-signaling, media to media.

A VPN tunnel key is required for tunnel communication, even if the data that's tunneled is unencrypted.

Procedure

1. Go to Integrations > VPN Tunnel Settings.
2. Click the Add button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN tunnel name</td>
<td>The descriptive name of the VPN tunnel.</td>
</tr>
<tr>
<td>Local IP address</td>
<td>The IP address of the network interface running the VPN tunnel service on</td>
</tr>
<tr>
<td></td>
<td>the local RealPresence DMA system.</td>
</tr>
<tr>
<td>Local port</td>
<td>The port on the local RealPresence DMA system used for all VPN communication.</td>
</tr>
<tr>
<td></td>
<td>This port can be the same as or different from the remote port.</td>
</tr>
<tr>
<td>Local VPN IP address</td>
<td>The virtual IP address on the local side that's unique to the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Internal VPN tunnel traffic will use this address, but it can be ignored for</td>
</tr>
<tr>
<td></td>
<td>all other contexts. It must be unique between the two systems.</td>
</tr>
<tr>
<td>Remote IP address</td>
<td>The IP address of the network interface running the VPN tunnel service on</td>
</tr>
<tr>
<td></td>
<td>the remote RealPresence DMA system.</td>
</tr>
<tr>
<td>Remote VPN IP address</td>
<td>The virtual IP address on the remote side that's unique to the tunnel.</td>
</tr>
<tr>
<td></td>
<td>Internal VPN tunnel traffic will use this address, but it can be ignored for</td>
</tr>
<tr>
<td></td>
<td>all other contexts. It must be unique between the two systems.</td>
</tr>
<tr>
<td>Remote port</td>
<td>The port on the remote RealPresence DMA system used for all VPN communication.</td>
</tr>
<tr>
<td></td>
<td>This port can be the same as or different from the local port.</td>
</tr>
<tr>
<td>Transport</td>
<td>The network transport the tunnel will use between the two systems.</td>
</tr>
<tr>
<td>TCP-Server</td>
<td>- The RealPresence DMA system that will initiate the TCP-based VPN tunnel</td>
</tr>
<tr>
<td></td>
<td>connection to a TCP-Client.</td>
</tr>
<tr>
<td>TCP-Client</td>
<td>- The RealPresence DMA system that will receive the TCP-based VPN tunnel</td>
</tr>
<tr>
<td></td>
<td>connection from a TCP-Server.</td>
</tr>
<tr>
<td>UDP</td>
<td>- Tunnel traffic will use UDP, the default transport mode for VPN tunnel</td>
</tr>
<tr>
<td></td>
<td>traffic. Communication will be attempted from both servers.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The type of encryption applied to VPN tunnel traffic if you have an</td>
</tr>
<tr>
<td></td>
<td>encryption license key. <strong>None</strong> is the only option if you don't have an</td>
</tr>
<tr>
<td></td>
<td>encryption license key.</td>
</tr>
</tbody>
</table>

4. Click **OK** to save the tunnel settings.

5. Click **Configure Remote DMA** and enter the following information:
   - **Remote management IP address** - the IP address of the management interface on the remote RealPresence DMA edge-configured system.
   - **Admin username** - The administrator username used to log into the management interface of the remote edge-configured system.
   - **Admin password** - The administrator password used to log into the management interface of the remote edge-configured system.

6. Click **OK** to automatically configure the VPN tunnel settings on the remote system.

The **VPN Status** column on the **VPN Tunnel Settings** page of both edge systems should display **Connected**, which means that the tunnel is not only established but that automated test network traffic is being successfully sent over the tunnel and back.
Manually Configure the VPN Tunnel Settings on the Remote RealPresence DMA System

When you create a VPN tunnel, you can configure the tunnel settings on one RealPresence DMA edge-configured system and then use the Configure Remote DMA option to automatically configure the remote edge system.

However, if your corporate firewall doesn't allow traversal of REST API traffic, you need to manually configure the VPN tunnel settings on the second (remote) edge system.

It's recommended that you add a VPN tunnel on the local system, then manually configure the VPN tunnel settings on the remote system at the same time.

When you configure the VPN tunnel settings on the second edge system, remember that some of the settings are reversed so you need to swap the values. These settings include the following:

- Local IP address and Remote IP address
- Local port and Remote port
- Local VPN IP address and Remote VPN IP address
- Transport TCP-Server and TCP-Client

The encryption settings must be identical.

Procedure

1. On the local edge system, go to Integrations > VPN Tunnel Settings.
2. Click the Add button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN tunnel name</td>
<td>The descriptive name of the VPN tunnel.</td>
</tr>
<tr>
<td>Local IP address</td>
<td>The IP address of the network interface running the VPN tunnel service on the local RealPresence DMA system.</td>
</tr>
<tr>
<td>Local port</td>
<td>The port on the local RealPresence DMA system used for all VPN communication. This port can be the same as or different from the remote port.</td>
</tr>
<tr>
<td>Local VPN IP address</td>
<td>The virtual IP address on the local side that's unique to the tunnel. Internal VPN tunnel traffic will use this address, but it can be ignored for all other contexts. It must be unique between the two systems.</td>
</tr>
<tr>
<td>Remote IP address</td>
<td>The IP address of the network interface running the VPN tunnel service on the remote RealPresence DMA system.</td>
</tr>
<tr>
<td>Remote VPN IP address</td>
<td>The virtual IP address on the remote side that's unique to the tunnel. Internal VPN tunnel traffic will use this address, but it can be ignored for all other contexts. It must be unique between the two systems.</td>
</tr>
<tr>
<td>Remote port</td>
<td>The port on the remote RealPresence DMA system used for all VPN communication. This port can be the same as or different from the local port.</td>
</tr>
</tbody>
</table>
Run the RealPresence DMA Edge Wizard on both VPN Tunnel Systems

After you create a VPN tunnel between two edge-configured systems, you can configure other default RealPresence DMA system communication settings by running the RealPresence DMA Edge Wizard on both edge systems.

When you run the wizard, you can create the default connections required for communication between the outside edge and inside edge systems and between the inside edge and a core-configured system. The default connections include a SIP peer, H.323 neighbor, and registration sharing, in addition to the default dial rules and access control lists that facilitate communication.

Procedure
1. On the outside edge system, go to Integrations > DMA Edge Wizard.
2. Complete the following fields:
   - Management host name of Core DMA - The management IP address of the inside edge system.
3. Complete the other required fields and click Next.
4. Click the Add button to add the inside edge system's signaling IP address.
5. Click OK, then click OK again to create the default connections between the outside edge system and the inside edge system.
6. On the inside edge system, go to Integrations > DMA Edge Wizard.
7. Complete the following fields:
   - Management host name of Core DMA - The management IP address of the RealPresence DMA core system.
   - Core DMA user name - The administrator user name used to log into the management interface of the core system.
   - Core DMA user password - The administrator password used to log into the management interface of the core system.
8. Complete the other required fields and click Next.
9. Click the Add button to add the core system's signaling IP address.
10. Click OK, then click OK again to create the default connections between the inside edge system and the core system.

Enable Outbound Calling Through a VPN Tunnel

After you set up a VPN tunnel and run the RealPresence DMA Edge Wizard on both your inside and outside edge systems, you need to create an external SIP peer and external gatekeeper on the inside edge system that point to the signaling address of the outside edge system.

You also need to revise the private dial plans for SIP and H.323 to enable outbound calling through the VPN tunnel.

**Procedure**

1. On the RealPresence DMA system inside your network, go to Integrations > External SIP Peers.
2. Add an external SIP peer with the following settings:
   - Next hop address - Enter the signaling IP address for the outside RealPresence DMA edge system.
   - Postliminary - Select Enabled > Use output format. Copy all parameters of original To headers.
   - In the Format field, select Use original request's To header.
3. Go to Integrations > External H.323 Gatekeepers.
4. Add an external H.323 gatekeeper with the following settings:
   - Address - Enter the signaling IP address for the outside RealPresence DMA edge system.
5. Go to Service Config > Dial Plan.
7. Under Dial Rules, select Resolve to external address and Resolve to ipaddress.
8. Click the Delete button, then click Yes to delete both rules.
9. Click the Add button.
10. In the Dial Rule tab, complete the fields as follows:
Enable Endpoint Provisioning through a VPN Tunnel

When you configure a VPN tunnel between your RealPresence DMA edge systems, you need to set up access proxy settings that enable the VPN tunnel to support provisioning.

Procedure

1. On the outside edge-configured system, go to Service Config > Access Proxy Settings.
2. Add an HTTPS proxy and specify 443 as the Public listening port.
3. Configure a next hop with the following settings:
   - **Type** - Request URI
   - **System** - Polycom Management System
   - **IP address** - IP address of the inside edge system.
   - **Port** - 9950 or an available port that access proxy on the inside edge system can listen on. Do not use port 443.
4. Add an LDAP proxy with the following settings:
   - **Public listening port** - 389
   - **Next hop address** - IP address of the inside edge-configured system.
   - **Next hop port** - 9951 or an available port that access proxy on the inside edge system can listen on. Do not use port 389.
5. Add an XMPP proxy with the following settings:
   - **Public listening port** - 5222
   - **Next hop address** - IP address of the inside edge-configured system
   - **Next hop port** - 9952 or an available port that access proxy on the inside edge system can listen on. Do not use port 5222.
6. On the inside edge-configured system, go to Service Config > Access Proxy Settings.
7. Add an HTTPS proxy and specify 9950 as the Public listening port.
8. Configure a next hop with the following settings:
   - **Type** - Request URI
   - **System** - Polycom Management System
9. Add an LDAP proxy with the following settings:
   - **Public listening port** - 9951
   - **Next hop address** - IP address of the RealPresence Resource Manager system
   - **Next hop port** - 389

10. Add an XMPP proxy with the following settings:
    - **Public listening port** - 9952
    - **Next hop address** - IP address of the RealPresence Resource Manager system
    - **Next hop port** - 5222

Related Links
VPN Tunnel Settings on page 237
Conference Manager
Configuration

Topics:

- Conference Settings
- Conference Templates
- Working with Conference Templates
- Template Priority
- About Cascading
- WebRTC Conferencing
- About Conference IVR Services
- IVR Prompt Sets
- Shared Number Dialing
- SIP Conference Factories
- Presence Publishing for Skype

This section provides an introduction to configuring conferences hosted by the Polycom RealPresence DMA system.
Conference Settings

Topics:

- Class of Service Overview
- Configure Conference Settings

Conference Settings define the default class of service and bit rate limits, a dialing prefix, and various default conference properties for the RealPresence DMA system.

If the system has been integrated with a Microsoft Lync 2013 or Skype for Business environment, you can also configure system-wide default settings related to presence publishing for Polycom conference contacts.

Related Links

View Conference Rooms on page 458
Add a Conference Room for a User on page 459
Edit a Conference Room for a User on page 465
Assign Conference Properties to a Group on page 479
Edit a User on page 453
User Roles on page 443

Class of Service Overview

You can specify a default class of service when you configure conference settings.

Class of service determines the priority of a device in a point-to-point call or the priority of the devices connected to a VMR (conference room), from bronze (lowest priority) to gold (highest priority).

The class of service of a user or group determines the class of service of an associated device. The class of service of a device determines the priority of that device's point-to-point call. Devices connected to a VMR inherit the class of service of the conference room for the duration of the call.

For example, if your device is assigned a bronze class of service and you attempt to dial a point-to-point call using a RealPresence DMA system saturated with gold- and silver-level conferences, the RealPresence DMA system will reject your call. However, if you use a device with a gold class of service to dial the same point-to-point call using the same RealPresence DMA system, the RealPresence DMA system will disconnect one of the silver-level devices to make room for your device.

Note: The Default maximum bit rate and Default minimum downspeed bit rate are the default values for point-to-point calls and conference room (VMR) calls.

Configure Conference Settings

Conference settings define the default conference properties for the RealPresence DMA system.

Procedure

1. Go to Service Config > Conference Manager Settings > Conference Settings.
2. Complete the fields described in the following table as needed.

### General Conference Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dialing prefix</td>
<td>Numeric dial string prefix for calling VMRs and VEQs. If you specify a prefix, the system uses it for both SIP and H.323 calls so that the same number can be dialed from both H.323 and SIP endpoints. If neighboring with a Polycom gatekeeper on which the Simplified Dialing service is enabled and uses a prefix of 9 (the default), don’t use 90-99. The neighbor gatekeeper recognizes the 9 as a known prefix and ignores the second digit. <strong>Caution:</strong> Changing the dialing prefix terminates any existing H.323 calls.</td>
</tr>
</tbody>
</table>

### Conference Defaults

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default class of service</td>
<td>The class of service assigned to a user or endpoint if the class of service is not specified at the endpoint, user, or group level. <strong>Note:</strong> The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Default maximum bit rate (kbps)</td>
<td>The maximum bit rate for a call if the maximum bit rate for the user or endpoint is not specified at the endpoint, user, or group level.</td>
</tr>
<tr>
<td>Default minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which a call can be reduced (downspeeded) if the minimum downspeed for the user or endpoint is not specified at the endpoint, user, or group level.</td>
</tr>
<tr>
<td>Default max total participants</td>
<td>Specifies the maximum conference size assigned to a conference room. <strong>Automatic</strong> (the default setting) uses the largest conference size supported by the MCU (or by all available MCUs if cascading is enabled) as the default maximum.</td>
</tr>
<tr>
<td>Default conference template</td>
<td>Default template used by the system.</td>
</tr>
<tr>
<td>Default MCU pool order</td>
<td>Default MCU pool order used by the system.</td>
</tr>
<tr>
<td>Default MCU selection algorithm</td>
<td>The process that the RealPresence DMA system uses when it selects MCUs from MCU pool orders: <strong>Prefer MCU in first MCU pool</strong> ensures that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on. <strong>Prefer MCU in first caller's site</strong> matches the MCU chosen for the call with the site to which the first caller's endpoint belongs.</td>
</tr>
</tbody>
</table>
### Conference Settings

#### Default conference room territory

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default conference room territory</td>
<td>The territory assigned to a user’s conference room if it is not specified at the user or conference room level. A conference room's territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). Up to three territories in a superclustered system can host conference rooms.</td>
</tr>
</tbody>
</table>

#### Default conference duration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default conference duration</td>
<td>Default maximum duration of a conference (in hours and minutes) or Unlimited (the maximum in this case depends on the MCU).</td>
</tr>
</tbody>
</table>

#### ID Generation Ranges

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated conference room IDs</td>
<td>The minimum and maximum values for auto-generated room IDs created for custom conference rooms. Values may be up to 18 digits long. The 18-digit limit applies only to generated IDs for custom conference rooms.</td>
</tr>
<tr>
<td>Generated conference room aliases</td>
<td>The minimum and maximum values for auto-generated conference room aliases created for custom conference rooms. Values may be up to 18 digits long. Values may be up to 18 digits long. The 18-digit limit applies only to conference room aliases for custom conference rooms.</td>
</tr>
<tr>
<td>Generated transient conference IDs</td>
<td>The minimum and maximum values for auto-generated transient conference IDs created for SIP conference factory conferences. Values may be up to 18 digits long. The 18-digit limit applies only to generated conference factory IDs for custom conference rooms.</td>
</tr>
</tbody>
</table>

#### MCU Selection

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum CIF ports required to start a conference on an MCU</td>
<td>The minimum number of available common intermediate format (CIF) video ports on an MCU that are required for the RealPresence DMA system to start a conference on the MCU.</td>
</tr>
<tr>
<td>Maximum percentage of CIF ports in use to start a conference on an MCU</td>
<td>The maximum percentage of CIF ports already in use on an MCU that determines if the RealPresence DMA system will start a conference on the MCU. The system won’t start a conference on an MCU if its percentage of ports already in use is equal to or above the maximum percentage you specify.</td>
</tr>
</tbody>
</table>
### Skype Experience

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roster cascade indicator</td>
<td>For Polycom conferences that cascade to Skype conferences, this setting specifies the name that displays in the Skype for Business client as the conference roster entry that corresponds to the Polycom conference. This setting confirms to the Skype client that a participant is valid and belongs in the conference (and should not be deleted). The value is 0-64 characters and can include the following: • Upper and lowercase letters • Spaces • ! % + - _ If the field is blank, the system uses conference-ID@domain, where the conference-ID is either the VMR or the Skype conference-ID (for RealConnect conferences).</td>
</tr>
</tbody>
</table>

### AS SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default resource priority namespace</td>
<td>In an assured services SIP (AS-SIP) environment, a local session controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. If your organization has implemented such a resource prioritization mechanism, set this value to the namespace being used for resource priority values. If the namespace being used is not listed, select Custom and enter the name in the box to the right of the list.</td>
</tr>
<tr>
<td>Default resource priority value</td>
<td>If your organization has implemented a resource prioritization mechanism, set this to the default priority value assigned to a conference if the specific conference room (VMR) doesn’t have a higher value. If using a custom namespace, enter the value in the box to the right of the list.</td>
</tr>
</tbody>
</table>

3. Click **Update** to save the settings.
Conference Templates

Topics:

- Standalone Templates
- Templates Linked to Polycom MCU Conference Profiles

The RealPresence DMA system uses conference templates to create conference rooms, which define a user's conference experience.

A conference template specifies a set of conference properties, such as the line (bit) rate and video display mode.

You can create a conference template in two ways:

- Specify the individual conference properties directly in the RealPresence DMA system, creating a standalone template independent of the profiles available on the system's Polycom MCUs.
- Link the template to a Polycom MCU conference profile that exists on some or all of the MCUs.

Either type of template can also include settings specific to Cisco Codian MCUs for deployments that include both Polycom MCUs and Cisco Codian MCUs.

Related Links

Add a Standalone Conference Template on page 251
Add a Linked Conference Template on page 266
Edit a Conference Template on page 267
Delete a Conference Template on page 267
Select a Video Frames Layout
View Conference Rooms on page 458
Add a Conference Room for a User on page 459
Edit a Conference Room for a User on page 465
Assign Conference Properties to a Group on page 479
Edit a User on page 453
User Roles on page 443

Standalone Templates

Standalone templates that you define in the RealPresence DMA system prevent you from having to ensure that the exact same MCU conference profiles exist on all MCUs.

You can specify the desired conference properties directly in the template.

When the RealPresence DMA system uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of the MCU's conference profiles.

When using a template not linked to a Polycom MCU conference profile, the RealPresence DMA system doesn't use the template's properties to limit its choice of an MCU. It selects the least used MCU in the selected MCU pool. Unsupported properties are ignored or degrade gracefully if necessary. For instance:

- If a conference set to a 4096 kbps line rate is forced to land on an MCU that doesn't support that value, the line rate falls back to 1920 kbps.
• If a conference with encryption enabled is forced to land on an MCU that doesn’t support encryption, the conference will be unencrypted.

To preferentially route conferences to certain MCUs, use MCU pool orders.

Templates Linked to Polycom MCU Conference Profiles

Linking a template to a Polycom MCU conference profile lets you access profile properties that are not currently available in a standalone template, since the MCU may offer more conference profile properties than standalone templates.

When you link a template with an MCU conference profile, the MCU's conference profile settings take priority over values set in the RealPresence DMA system template.

When you link a template to a conference profile, consider the following details:

• You must ensure that the conference profile exists on the MCUs you want to use with that template and that the profile's settings are the same on all of the MCUs.

• If the Polycom MCU conference profile has recording enabled, the RealPresence DMA system doesn’t recognize this and rejects attempts to start recording via the API. To enable recording control via the API, use a standalone conference template with recording enabled.

• If you select the **Chairperson required** option for a conference room on the RealPresence DMA system, this option is ignored if the conference template is linked to a Polycom MCU conference profile.

• When you link to a Polycom MCU conference profile that uses an interactive voice response (IVR) service, and you want the IVR service to prompt for a chairperson passcode, you must select the following settings on the Polycom MCU:
  - **Conference Requires Chairperson** in the IVR properties of the profile
  - **Enable Chairperson Messages** in the properties for the specific IVR service the Polycom MCU uses
    
    If the IVR service is not configured to prompt for passcodes, callers are not prompted even if the conference has a conference or chairperson passcode.

When the RealPresence DMA system uses a profile-based conference template, the system uses the MCU pool order rules to find an MCU that has that profile. The system then selects the least-used MCU in the pool that has that profile.

If none of the MCUs in the pool have that profile, the system selects the least-used MCU in the pool and does one of the following:

• If the system selected a Cisco Codian MCU, it uses the Codian-specific settings of the specified template.

• If the system selected a Polycom MCU, it falls back to its default conference template. If the default template happens to be linked to a profile that this MCU doesn't have, the system falls back to its built-in conference properties settings.
Working with Conference Templates

Topics:

- View the Conference Templates List
- Add a Standalone Conference Template
- Add a Linked Conference Template
- Edit a Conference Template
- Delete a Conference Template

The following sections describe the conference templates tasks you can perform.

View the Conference Templates List

You can view the conference templates list for priority and descriptive information about each conference template.

The RealPresence DMA system comes with a Factory Template that has a default set of conference parameters. You can edit that template and create additional templates.

Procedure

» Go to Service Config > Conference Manager Setting > Conference Templates.

The following table describes the fields in the Conference Templates list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The priority ranking of the template.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the template.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the template.</td>
</tr>
</tbody>
</table>

Add a Standalone Conference Template

You can add a standalone conference template to specify conference properties.

When the RealPresence DMA system uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of the MCU's conference profiles.

The Common Settings apply to all PolycomMCUs and Cisco Codian MCUs.

Procedure

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. Select the Add button.
3. Specify the conference template settings as described in the following table:
### Common Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the template (up to 50 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the conference template (up to 50 characters).</td>
</tr>
</tbody>
</table>

**WebRTC**

Select one of the following options:

- **No WebRTC** - This template excludes WebRTC capability. WebRTC participants are disconnected if they attempt to connect to conferences using this conference template.

- **WebRTC with MCUs only** - Conferences using this template accept WebRTC, SIP, and H.323 participants. The system promotes these conferences to a WebRTC-capable MCU as soon as the first participant connects.

- **WebRTC with mesh only** - Conferences using this template only accept WebRTC participants. All non-WebRTC participants are disconnected. Mesh only conferences allow up to three participants; if a fourth participant attempts to join, the new participant is disconnected.

- **WebRTC with MCUs or mesh** - Conferences using this template accept WebRTC participants. A WebRTC-only conference of up to three participants runs in mesh mode; if a fourth participant or non-WebRTC participant joins, the conference is automatically promoted to a WebRTC-capable MCU.

### Polycom MCU General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom MCU Profile Settings</td>
<td></td>
</tr>
<tr>
<td>Use existing profile</td>
<td>Links this template to the profile you select in the Polycom MCU profile name field. Only available when you select the No WebRTC option in Common Settings. Polycom recommends leaving this box unchecked and specifying conference properties directly.</td>
</tr>
<tr>
<td>Polycom MCU profile name</td>
<td>Identifies the profile to which this template is linked. The list contains the names of all the profiles available on the currently connected MCUs. If a profile is only available on some of the connected MCUs, its entry shows how many of the MCUs have that profile. The system will put conferences using this template on the least used MCU that has this profile. If there is none, it selects the least-used MCU and either uses the Codian-specific settings if it selected a Cisco Codian MCU or falls back to the default conference template if it selected a Polycom MCU.</td>
</tr>
</tbody>
</table>
### Conference Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference mode</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>AVC only</strong> - Standard video conferencing mode supporting the H.264 advanced video coding (AVC) compression standard. In an AVC conference, the MCU transcodes the video stream to each device in the conference to provide an optimal experience, based on its capabilities.</td>
</tr>
<tr>
<td></td>
<td>This is the only mode that supports the use of Polycom MCU conference profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SVC only</strong> - Video conferencing mode supporting the Annex G extension of the H.264 standard, known as H.264 scalable video coding (SVC). An SVC video stream consists of a base layer stream that encodes the lowest available quality representation plus optional enhancement layer streams that each provide an additional quality improvement. The MCU passes the video streams from each device to each device.</td>
</tr>
<tr>
<td></td>
<td>The number of enhancement layer streams sent to a device can be tailored to fit the bandwidth available and device capabilities.</td>
</tr>
<tr>
<td></td>
<td>SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. Select this setting to disable most of the other template settings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mixed AVC and SVC</strong> - Enables both AVC-only endpoints and endpoints supporting SVC to join the conference. If the selected MCU doesn’t support SVC, the conference is started in AVC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the MCU supports SVC but not mixed mode, the conference fails to start.</td>
</tr>
<tr>
<td>Conference mode experience</td>
<td>For mixed conference mode, this option specifies the video experience optimization strategy the MCU should implement. The experience optimization strategy determines the quality of the video streams that SVC participants receive from AVC participants.</td>
</tr>
<tr>
<td></td>
<td>See the documentation for your Polycom MCU for detailed data regarding the resolutions each experience setting supports for various ranges of line rate.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All AVC callers must be capable of sending at a line rate available for the experience setting. SVC participants receive the same stream quality from all AVC endpoints, regardless of their individual capabilities.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cascade for bandwidth</td>
<td>Enables conferences using this template to span Polycom MCUs to conserve network bandwidth. Cascading for bandwidth requires site topology information, which the RealPresence DMA system can get from a RealPresence Resource Manager system. You can also create the site topology information. This option and the Cascade for size option are mutually exclusive.</td>
</tr>
<tr>
<td>Cascade for size</td>
<td>Enables conferences using this template to span Polycom MCUs to achieve conference sizes larger than a single MCU can accommodate. This option and the Cascade for bandwidth option are mutually exclusive.</td>
</tr>
<tr>
<td>Cascade for SVC</td>
<td>This option is currently not supported.</td>
</tr>
</tbody>
</table>
| Video switching (VSW)   | Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen while the current speaker sees the previous speaker. If this mode is enabled:  
  ▪ The minimum line rate available is 768 kbps.  
  ▪ All endpoints must connect at the same line rate, and those that don’t support the specified line rate are connected in voice-only mode.  
  ▪ The video clarity, layout, and skins settings are not available.  
  ▪ LPR is automatically turned off, but can be turned back on.  
If this option is not selected, conferences using this template are in continuous presence (CP) mode. This means that the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. |
| H.264 high profile      | Sets a VSW conference to use Polycom’s bandwidth-conserving H.264 High Profile codec, which was previously only supported in continuous presence mode. If selected, all endpoints in the conference must support H.264 High Profile. The endpoints will only connect in audio mode if they don’t connect at the conference’s exact line rate and resolution. |
| Resolution              | Offers various resolution settings, some of which are only available on Polycom MCUs with MPM+, MPMx, or MPMRx cards. Only available if Video switching is selected.                                              |
| Line rate               | The maximum bit rate at which endpoints can connect to conferences using this template. If Video switching is selected, the minimum line rate is 768 kbps.                                                        |
### Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Select one of the following options to specify the media encryption setting for conferences using this template:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>No encryption</strong> - All endpoints join unencrypted</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Encrypt when possible</strong> - Endpoints supporting encryption join encrypted; others join unencrypted.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Encrypt all</strong> - Endpoints supporting encryption join encrypted; others can’t join.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> VMR dial-outs to H.323 endpoints from an encrypted RealPresence DMA system conference are unsupported and won’t connect.</td>
</tr>
<tr>
<td></td>
<td>Refer to the MCU’s <em>Administrator’s Guide</em> for information about media encryption (SRTP).</td>
</tr>
<tr>
<td>Packet loss compensation (LPR and DBA)</td>
<td>Enables lost packet recovery (LPR) and dynamic bandwidth allocation (DBA) for conferences using this template.</td>
</tr>
<tr>
<td></td>
<td>LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission. DBA allocates</td>
</tr>
<tr>
<td></td>
<td>the bandwidth needed to transmit the additional packets.</td>
</tr>
<tr>
<td>Exclusive content mode</td>
<td>When checked, this option blocks participants from interrupting the current content stream.</td>
</tr>
<tr>
<td></td>
<td>The participant who is actively broadcasting content must stop sharing before anyone else can share content.</td>
</tr>
<tr>
<td>Enable FECC</td>
<td>When checked, enables far end camera control (FECC) for conference participants.</td>
</tr>
<tr>
<td>FW NAT keep alive</td>
<td>Select the check box to specify that when the MCU receives calls through a session border controller (SBC), the MCU should send media stream</td>
</tr>
<tr>
<td></td>
<td>keep-alive messages to the SBC at the chosen interval.</td>
</tr>
<tr>
<td>Interval (seconds)</td>
<td>Specify how often to send keep-alive messages.</td>
</tr>
<tr>
<td>TIP compatibility</td>
<td>Enables compatibility with Cisco’s Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences</td>
</tr>
<tr>
<td></td>
<td>can include both endpoints that don’t support TIP and Cisco TelePresence System (CTS) endpoints. If <strong>Prefer TIP</strong> is selected, TIP content</td>
</tr>
<tr>
<td></td>
<td>is used for endpoints that support TIP, and non-TIP content is used with non-TIP endpoints.</td>
</tr>
<tr>
<td></td>
<td>Requires minimum line rate of 1024 kbps and HD resolution (720 or better).</td>
</tr>
</tbody>
</table>
### Field

**MS AVMCU cascade mode**

If integrated with a Microsoft Skype for Business environment, these options control the behavior of the cascade link with the Skype for Business AVMCU:

- **Resource optimized** - The cascade link between the RealPresence DMA system and the Skype for Business server's AVMCU is limited to SD video resolutions to conserve MCU resources.

- **Video optimized** - The cascade link between the RealPresence DMA system and the Skype for Business server's AVMCU is capable of HD video resolutions, increasing MCU resource usage.

**Enable MS panoramic layout**

If integrated with a Microsoft environment (Lync 2013, Skype for Business 2015, or Office 365), enables a Polycom MCU to stream a panoramic layout from telepresence rooms or multiple non-Microsoft participants to Microsoft clients.

**Note:** This option applies to on-premise and service provider deployment models.

**Font for text over video (MPMx or newer)**

Specifies the font type for text displayed to participants in a conference. If **Default** is selected, the system will display Heiti if a Chinese language is configured.

**Note:** This property only applies when the MCU is configured for multilingual operation with Chinese (Simplified or Traditional) selected.

### Polycom MCU Gathering Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable gathering</strong></td>
<td>Enables the gathering phase for conferences using this template. The gathering phase is a time period, which is configurable on the MCU, at the beginning of a conference when people are connecting. During this time, a slide displays that contains conference information, including a list of participants and some information you can specify here. <strong>Note:</strong> Not available if <strong>Video switching</strong> is selected.</td>
</tr>
<tr>
<td><strong>Displayed language</strong></td>
<td>The language in which the gathering page is displayed.</td>
</tr>
<tr>
<td><strong>Access number 1</strong></td>
<td>Optional access numbers to display on the gathering phase slide.</td>
</tr>
<tr>
<td><strong>Access number 2</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Info1, Info2, Info3
Optional free-form text fields to display on the gathering phase slide.

Refer to the MCU’s Administrator’s Guide to see an example of the slide and the location and appearance of these fields.

On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint.

### Polycom MCU Video Quality

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>People Video Definition</td>
<td></td>
</tr>
<tr>
<td>Video quality</td>
<td>Select of the following video optimizations:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Motion</strong> - higher frame rate</td>
</tr>
<tr>
<td></td>
<td>- <strong>Sharpness</strong> - higher resolution</td>
</tr>
<tr>
<td></td>
<td>Not available if Conference mode is set to SVC only.</td>
</tr>
<tr>
<td>Max resolution</td>
<td>Enables you to choose a resolution setting that limits the conference to no more than that resolution regardless of the line rate and resolution capabilities of the MCU and endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>Auto</strong> (the default) imposes no limit.</td>
</tr>
<tr>
<td></td>
<td>Not available if Conference mode is set to SVC only.</td>
</tr>
<tr>
<td>Video clarity</td>
<td>Enables a video enhancement process that improves clarity, edge sharpness, and contrast on streams with resolutions up to and including SD.</td>
</tr>
<tr>
<td></td>
<td>Not available if Video switching is selected or if Conference mode is set to SVC only.</td>
</tr>
<tr>
<td>Auto brightness</td>
<td>Enables the automatic balancing of brightness levels to compensate for an endpoint sending a dim image.</td>
</tr>
<tr>
<td></td>
<td>Not available if Conference mode is set to SVC only.</td>
</tr>
</tbody>
</table>

### Content Video Definition
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content settings</td>
<td>Select one of the following transmission modes for the content channel:</td>
</tr>
<tr>
<td></td>
<td>• Graphics - lowest bit rate for basic graphics</td>
</tr>
<tr>
<td></td>
<td>• High-resolution graphics - higher bit rate for better graphics resolution</td>
</tr>
<tr>
<td></td>
<td>• Live video - the content channel is used for live video</td>
</tr>
<tr>
<td></td>
<td>• Customized content rate - allows you to specify a Content rate</td>
</tr>
<tr>
<td></td>
<td>A higher bit rate for the content channel reduces the bit rate for the people channel.</td>
</tr>
<tr>
<td>AS SIP content</td>
<td>Enables content sharing using the AS-SIP protocol security features.</td>
</tr>
<tr>
<td>Multiple content resolutions</td>
<td>Enables content sharing over multiple video streams. When selected, you can choose which protocols to use for each stream with the Transcode to setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is only available when:</td>
</tr>
<tr>
<td></td>
<td>• Conference mode is set to AVC only.</td>
</tr>
<tr>
<td></td>
<td>• TIP compatibility is set to either None or Video Only.</td>
</tr>
<tr>
<td>Transcode to</td>
<td>This option is enabled when you select the Multiple content resolutions check box. Choose which protocols to use for each stream of content.</td>
</tr>
<tr>
<td>TIP encoder</td>
<td></td>
</tr>
<tr>
<td>TIP Content Resolution</td>
<td></td>
</tr>
<tr>
<td>Content protocol</td>
<td>Select one of the following content channel protocol options:</td>
</tr>
<tr>
<td></td>
<td>• Use H.263</td>
</tr>
<tr>
<td></td>
<td>• Use H.263 &amp; H.264 auto selection</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 cascade and SVC optimized</td>
</tr>
<tr>
<td></td>
<td>• Use H.264 HD</td>
</tr>
<tr>
<td>H.264 high profile</td>
<td>Enables the H.264 High Profile set of capabilities for the content channel, which enables additional compression efficiency and allows for higher resolutions to use the same bandwidth.</td>
</tr>
<tr>
<td>Send content to legacy endpoints</td>
<td>Enables endpoints that don't support H.239 to receive the content channel over the video (People) channel.</td>
</tr>
<tr>
<td></td>
<td><strong>Not available if Video switching or Same layout is selected, or if Telepresence mode is On.</strong></td>
</tr>
</tbody>
</table>
Enable MS RDP content

When selected, enables the RealPresence DMA system to start conferences based on this template only on Modular MCUs (MMCU) that have sufficient soft blade resources.

MMCUs may be configured with an RDP translator that converts H.264 content shared from a standard endpoint to RDP content to deliver to a Skype ASMCU. Likewise, when a Skype client shares RDP content, the RDP translator delivers H.264 content to the MMCU.

If not selected, the system considers all MCUs within the MCU pool order when starting a conference. However, even if the system selects an MMCU configured with an RDP translator, RDP content will not be delivered to or from Skype clients.

If an MCU failover occurs, video is automatically reconnected, but content is not re-established. The Skype conference or client must re-initiate content.

Note: This option can be used in place of a separate Polycom ContentConnect gateway solution.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation mode</td>
<td>Enables a conference to change to lecture mode when the current speaker speaks for 30 seconds. When another participant starts talking, it returns to the previous video layout.</td>
</tr>
<tr>
<td></td>
<td>Not available if Video switching or Same layout is selected, or if Telepresence mode is On.</td>
</tr>
<tr>
<td>Same layout</td>
<td>Forces the selected layout on all participants. Personal selection of the video layout is disabled.</td>
</tr>
<tr>
<td></td>
<td>Not available if Presentation mode or Video switching is selected, or if Telepresence mode is On.</td>
</tr>
<tr>
<td>Lecturer view switching</td>
<td>When in lecture mode, enables the lecturer’s view to automatically switch among participants (if the number exceeds the number of windows in the layout) while the lecturer is talking.</td>
</tr>
<tr>
<td></td>
<td>Not available if Same layout is selected or Telepresence mode is On.</td>
</tr>
<tr>
<td>Auto layout</td>
<td>When checked, lets the system select the video layout based on the number of participants in conference.</td>
</tr>
<tr>
<td></td>
<td>If not checked, you can select a specific layout (below).</td>
</tr>
<tr>
<td></td>
<td>Not available if Video switching is selected or Telepresence mode is On.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Layout</td>
<td>With <strong>Auto layout</strong> unchecked, you can select the number and arrangement of video frames. Option is not available if <strong>Video switching</strong> is selected.</td>
</tr>
<tr>
<td>Telepresence mode</td>
<td>Select one of the following support options for telepresence conference rooms joining the conference:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong> (default) - A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins. This is the recommended setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On</strong> - Telepresence mode is on, regardless of whether a telepresence endpoint is present.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off</strong> - Telepresence mode is off, regardless of whether a telepresence endpoint is present.</td>
</tr>
<tr>
<td>Note:</td>
<td>The system flag <strong>ITP_CERTIFICATION</strong> must be set to <strong>YES</strong>. Refer to the information about system flags in the MCU's Administrator's Guide.</td>
</tr>
<tr>
<td>Telepresence layout mode</td>
<td>Select one of the following layout options for telepresence conferences:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong> - Layout is controlled manually by a conference operator using the multipoint layout application (MLA) interface.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Continuous Presence</strong> - Tells the MLA to generate a multipoint view (standard or custom).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Room Switch</strong> - Tells the MLA to use voice activated room switching (VARS). The speaker's site is the only one seen by others.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Speaker Priority</strong> - Ensures that the current speaker is always displayed in the video layout. The previous speakers are also displayed if there is room in the layout. In this mode, each endpoint in the conference reserves screens for displaying the active speaker in the largest video layout cell available.</td>
</tr>
<tr>
<td>Note:</td>
<td>Not available if <strong>Telepresence mode</strong> is <strong>Off</strong>. Refer to the Polycom Multipoint Layout Application User Guide for more information about layouts</td>
</tr>
</tbody>
</table>

### Polycom MCU Audio Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo suppression</td>
<td>Enables the MCU to detect and suppress echo.</td>
</tr>
<tr>
<td>Keyboard noise suppression</td>
<td>Enables the MCU to detect and suppress keyboard noise.</td>
</tr>
<tr>
<td>Audio clarity</td>
<td>Improves the voice quality for PSTN endpoint conferences.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Mute participants except lecturer</th>
<th>Enables the MCU to automatically mute all participants except the lecturer upon connection to the conference.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoiseBlock</td>
<td>Enables the MCU to automatically detect and mute endpoints that have a noisy audio channel.</td>
</tr>
<tr>
<td>Speaker change threshold (seconds)</td>
<td>Allows you to configure the amount of time the MCU requires a participant to speak continuously until becoming the speaker. The default Auto setting is 3 seconds.</td>
</tr>
<tr>
<td>Polycom MCU Skins</td>
<td>Enables you to choose the display appearance (skin) for conferences using this template. Not available if Telepresence mode is On or Video switching is enabled.</td>
</tr>
</tbody>
</table>

#### Polycom MCU Conference IVR

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Override default conference IVR service | Links this template to the specific conference IVR service selected in the list below.  
  **Note:** The Polycom MCU conference IVR service is separate and distinct from the RealPresence DMA system's SIP-only shared number dialing feature. 
  
  For most purposes, this option should not be selected. This option enables the system to choose one of two defaults, depending on whether callers need to be prompted for passcodes. If you do select this option, be sure the IVR service you select is appropriate for the users who will use this template. |
| Conference IVR service          | The list contains the names of all the conference IVR services available on the currently connected MCUs. If an IVR service is only available on some of the connected MCUs, its entry shows how many of the MCUs have that IVR service (for example, 2 of 3). 
  
  The system will put conferences using this template on the least used MCU that has the selected conference IVR service. If there are none, it falls back to the default conference IVR service. |
### Conference requires chairperson

When checked, conferences based on this template won’t start unless a chairperson joins (callers arriving earlier are placed on hold). The conference may end when the last chairperson leaves, depending on the MCU configuration.

This option is ignored if the user doesn’t have a chairperson passcode.

For enterprise users, chairperson passcodes can come from the Active Directory, but you can override the Active Directory value.

For local users, you can add or change chairperson passcodes when you create or edit the users.

**Note:** If this option is enabled and this template is used for a Polycom RealConnect conference, the Skype for Business presenter acts as the chairperson for that conference.

### Terminate conference after chairperson drops

If this template is used for a conference with a chairperson passcode and the **Conference requires chairperson option is selected**, you can select this option if you want the conference to terminate when the last chairperson leaves the conference.

A message plays to the remaining participants informing them that the chairperson has left the conference.

### Polycom MCU Site Names

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Display mode               | Overlays the endpoint display name on each video participant’s display in a Continuous Presence conference:  
  - **Auto** - Display site names only when the layout changes.  
  - **On** - Always display site names.  
  - **Off** - Do not display site names (default).                                                                                                                                 |
| Font size                  | Controls the font size for the site name text. The default value is 12.                                                                                                                                 |
| Color                      | Controls the font and background color.  
  When you select one of the **Polycom MCU Skins** with a background image, there are more color choices available for selection.                                                                              |
<p>| Text color                 | Controls the text color.                                                                                                                                                                                    |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display position</td>
<td>Controls the position of the text within the video participant's display with preset or custom locations. The value changes to <strong>Custom</strong> if you use the <strong>Horizontal position</strong> or <strong>Vertical position</strong> sliders to change the position to one that is not defined by a preset value.</td>
</tr>
<tr>
<td>Horizontal position</td>
<td>Allows you to manually control the horizontal position of the site name text.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Allows you to manually control the vertical position of the site name text.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>When you choose one of the <strong>Polycom MCU Skins</strong> with a background image, you can move this slider to control the transparency of the site name font background.</td>
</tr>
</tbody>
</table>

**Polycom MCU Recording**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record conference</td>
<td>Select one of the following conference recording setting for this template:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong> - Recording isn't available for conferences using this template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Immediately</strong> - Recording begins automatically when the conference starts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Upon Request</strong> - Recording can be initiated manually by the chairperson or an operator.</td>
</tr>
<tr>
<td></td>
<td>Conference recording requires a Polycom RealPresence Media Suite or Polycom Capture Server recording system and an MCU that supports recording.</td>
</tr>
<tr>
<td>Dial out recording link</td>
<td>Select a specific recording link or the MCU's default.</td>
</tr>
<tr>
<td></td>
<td>The list contains the names of all recording links available on the connected MCUs, with the number of MCUs that have the link shown in parentheses.</td>
</tr>
<tr>
<td>Audio only</td>
<td>When checked, limits recording to the audio channel of the conference.</td>
</tr>
<tr>
<td>Indication of recording</td>
<td>When checked, displays a red dot recording indicator in the upper left corner of the video layout.</td>
</tr>
<tr>
<td>Play recording message</td>
<td>Select the check box to play a recording message.</td>
</tr>
</tbody>
</table>
## Polycom MCU Indications

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
<td>Select an option from the drop-down menu to set the display position of the indication icons group.</td>
</tr>
<tr>
<td>Recordings</td>
<td>Enables the recording icon to display when a recording is in progress.</td>
</tr>
</tbody>
</table>

### Media type indications

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio participants</td>
<td>Select the check box to enable the Audio Participants icon.</td>
</tr>
<tr>
<td>Video participants</td>
<td>Select the check box to enable the Video Participants icon.</td>
</tr>
</tbody>
</table>

### Display mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent</td>
<td>Enables the MCU to display the icon permanently when audio or video participants connect.</td>
</tr>
<tr>
<td>On participant join or leave</td>
<td>Enables the MCU to display the icon for a short period of time when the number of audio or video participants changes.</td>
</tr>
<tr>
<td>Duration</td>
<td>Allows you to select the length of time that the icon is visible when a participant joins or leaves the conference.</td>
</tr>
<tr>
<td>Network Quality</td>
<td>Enables the MCU to display the Network Quality icon, which indicates the network quality for any individuals experiencing significant packet loss.</td>
</tr>
</tbody>
</table>

## Polycom MCU Message Overlay

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable message overlay</td>
<td>Select the check box to enable Message Overlay (disabled by default).</td>
</tr>
<tr>
<td>Content</td>
<td>Enter the message text.</td>
</tr>
<tr>
<td></td>
<td>The message text can be up to 50 unicode characters.</td>
</tr>
<tr>
<td>Font size</td>
<td>Configure the font size of the message text.</td>
</tr>
<tr>
<td></td>
<td>The default is 24 points.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In some languages, for example Russian, when a large font size is selected, both rolling and static messages may be truncated if the message length exceeds the resolution width.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color</td>
<td>Select the color and background of the message text. Default is white text on a red background.</td>
</tr>
<tr>
<td>Vertical position</td>
<td>Move the slider right to move the vertical position of the displayed text downward within the video layout.</td>
</tr>
<tr>
<td></td>
<td>Move the slider left to move the vertical position of the displayed text upward within the video layout.</td>
</tr>
<tr>
<td>Background transparency</td>
<td>Move the slider to the left to decrease the transparency of the background of the message text. 0 indicates no transparency (solid background color).</td>
</tr>
<tr>
<td></td>
<td>Default is 50.</td>
</tr>
<tr>
<td>Display repetition</td>
<td>Configure the number of times that the text message display repeats. Default is 3.</td>
</tr>
<tr>
<td>Display speed</td>
<td>Select whether the message is static or moves across the screen. If moving, choose the movement speed. The default speed is <strong>Slow</strong>.</td>
</tr>
</tbody>
</table>

### Cisco Codian

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floor and chair control</td>
<td>Specifies how much control conference participants may have:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Do not allow floor or chair control</strong> - Participants have no control.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Allow floor control only</strong> - A participant may take the floor. Everyone sees that participant's video full-screen.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Allow floor and chair control</strong> - A participant may also take the chair. The chair can designate whose video everyone sees full-screen. The chair can also disconnect participants.</td>
</tr>
<tr>
<td></td>
<td>This setting only works in H.323 conferences and if H.243 Floor and Chair Control is enabled on the MCU. All endpoints must support H.243 chair control.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatic lecture mode (4.1)</td>
<td>Enables the MCU to put a conference into lecture mode, either immediately or after the speaker has been talking for the selected interval. In lecture mode, the lecturer (speaker) is displayed full-screen to the other participants. The lecturer sees the normal continuous presence view.</td>
</tr>
<tr>
<td>Layout control via FECC/DTMF</td>
<td>Enables participants to change their individual layouts using far end camera control, with or without fallback to touchtone commands for endpoints that don't support FECC.</td>
</tr>
<tr>
<td>Mute in-band DTMF (4.1)</td>
<td>Specifies whether the MCU mutes participants' in-band DTMF (touchtones) so that other participants don't hear them.</td>
</tr>
<tr>
<td>Allow DTMF *6 to mute audio (4.1)</td>
<td>Enables conference participants to mute themselves using the *6 touchtone command.</td>
</tr>
<tr>
<td>Content channel video</td>
<td>Enables the conference to support a second video stream for content. Only available if Content Status is enabled on the MCU.</td>
</tr>
<tr>
<td>Transmitted content resolutions (4.1)</td>
<td>Specifies the aspect ratio used for the content channel. If Allow all resolutions is selected, endpoints with a 16:9 aspect ratio receive that, and others receive 4:3.</td>
</tr>
<tr>
<td>Conference custom layout</td>
<td>Enables the Conference layout desired setting, where you can select the number and arrangement of video frames by clicking the image.</td>
</tr>
<tr>
<td>Conference layout desired</td>
<td>If the Conference custom layout option is enabled, you can select the number and arrangement of video frames by clicking the image. A small representation of the layout you choose displays here.</td>
</tr>
</tbody>
</table>

4. Select OK.

The new template displays in the Conference Templates list.

Related Links
Conference Templates on page 249
Shared Number Dialing on page 278

Add a Linked Conference Template
You can add a conference template that's linked to a Polycom MCU conference profile.
You can choose conference profiles from MCUs that have been added to the RealPresence DMA system.
Procedure
1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. Select the Add button.
3. In the Add Conference Template dialog, specify all the conference properties for this template:
   a. In Common Settings, enter a template name and description.
   b. Select Polycom MCU General Settings.
   c. Select Use existing profile and select the one you want from the Polycom MCU profile name list.

The list contains the profiles available on the Polycom MCUs that have been added to the RealPresence DMA system. If no MCUs have been added, the list is disabled.
4. Select OK.

The new template displays in the Conference Templates list.

Related Links
Conference Templates on page 249
Shared Number Dialing on page 278

Edit a Conference Template

Editing an existing conference template is not supported.

If you need to make changes to an existing conference template, you need to delete the template and create a new one with the revised settings.

Related Links
Conference Templates on page 249
Shared Number Dialing on page 278

Delete a Conference Template

You can remove a conference template from the system.

Procedure
1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. In the Conference Templates list, select the template you want to delete, and click Delete.
3. When asked to confirm that you want to delete the template, click Yes.

Any conference rooms or enterprise groups that used the template are reset to use the system default template.

Related Links
Conference Templates on page 249
Shared Number Dialing on page 278
Template Priority

Topics:

- Change a Conference Template’s Priority

A user, either local or enterprise, has one or more conference rooms. Each room may either use the system’s default template or a specifically assigned template. Generally, most conference rooms use the default template.

An enterprise user can be associated with multiple enterprise groups, and each group may or may not have a specifically assigned template.

You can rank the conference templates by priority, so that the system knows which template to use when the user is associated with more than one.

When someone dials into a conference room, the system uses the following rules, in order of importance, to determine which template to use for the conference:

1. If the conference room has a specifically assigned template that is not the system default, use that template.
2. If the user associated with the conference room belongs to one or more enterprise groups that have specifically assigned templates, use the template with the highest priority.
3. Otherwise, use the system default conference template.

Change a Conference Template’s Priority

You can control the priority of conference templates. This allows you to tell the system which template it should use when a user is associated with more than one.

Procedure

1. Go to Service Config > Conference Manager Settings > Conference Templates.
2. On the Conference Templates list, select the template whose priority you want to change.
3. In the Actions list, select Move Up or Move Down, depending on whether you want to increase or decrease the template’s priority ranking.
   When a user is associated with multiple templates, the system uses the highest priority template. Polycom recommends moving the system default template to the bottom of the list.
4. Repeat until the template has the desired ranking.
About Cascading

Topics:

- Cascading for Bandwidth
- Cascading for Size

One of the conference features you can optionally enable in a template is cascading, which allows a conference to span multiple Polycom MCUs.

Only one of the two forms of cascading can be enabled at once:

- Cascading for Bandwidth
- Cascading for Size

The cascade links between MCUs use H.323 or SIP signaling. SIP signaling is used in the following situations:

- When the conference is limited to SVC endpoints.
- When one of the MCUs doesn’t support H.323.
- When the conference template settings specify to Cascade for SVC.

For cascade for size and bandwidth calls to work, you need to configure each RealPresence Collaboration Server that will be used for cascading to point to the RealPresence DMA system as the H.323 gatekeeper. You also need to add a dial rule with the Resolve to service prefix action.

Cascading for Bandwidth

Cascading for bandwidth uses a hub-and-spoke configuration; each cascaded MCU is only one link away from the hub MCU that hosts the conference.

To host the conference, the RealPresence DMA system chooses the same MCU that it would have chosen in the absence of cascading.

Cascading a conference across multiple MCUs to conserve bandwidth is especially useful when using WAN links. Participants can connect to MCUs that are geographically near them, reducing network traffic between sites to a single link to each MCU.

The RealPresence DMA system uses site topology information to cascade conferences for bandwidth. If you have a RealPresence Resource Manager system in your network, you can integrate your RealPresence DMA system with the RealPresence Resource Manager system to obtain its site topology data. You can then enable cascaded-for-bandwidth conferences with the following steps:

- On the RealPresence Resource Manager system, create site topology data defining the territories, sites, site links, and MPLS clouds in your network, and the subnets in each site.
- On the RealPresence DMA system, integrate with the RealPresence Resource Manager system to obtain its site topology data.
- On the RealPresence DMA system, enable cascading for bandwidth in some or all of your conference templates.

If you don’t have a RealPresence Resource Manager system, you must define your site topology in the RealPresence DMA system instead of importing it.
Processing a Cascaded-for-Bandwidth Call

Once a conference with cascading for bandwidth enabled has started, the RealPresence DMA system uses the site topology information to route callers to the nearest eligible MCU (using the pool order applicable to the conference) that has available capacity:

- If the caller is in a site that contains one or more MCUs, the system selects an MCU in that site (it selects the same MCU that it would have chosen in the absence of cascading).
- If the caller is in a site that doesn't contain MCUs, the system looks for MCUs in sites that only have a direct network path to the caller's site (not through a cloud) and selects one.
- If there are no MCUs in sites that only have a direct network path to the caller's site, the system looks for MCUs in sites that are connected to the caller's site through a cloud and selects one.
- If an MCU belongs to an MCU pool, the DMA system selects an MCU that meets the requirements of the selection process from the highest priority pool within the pool order.

If a selected MCU is new to the conference, the RealPresence DMA system creates the cascade link to the hub MCU hosting the conference. The cascade link bandwidth matches the conference setting.

Cascaded conferences can have conference passcodes and can be Polycom Conferencing for Outlook (calendared) conferences.

Cascading for Size

Cascading for size makes it possible for a conference to contain many more participants than any single MCU could support and differs from cascading for bandwidth in two primary ways:

- Cascading for size doesn’t use site topology information to choose additional MCUs for a conference.
- Cascading for size supports a second level of cascade links so that a cascaded MCU can be either one link away (this is a spoke MCU) from the hub MCU hosting the conference or two links away (a leaf MCU linked to a spoke MCU).

To host a cascade-for-size conference, the RealPresence DMA system chooses the same MCU that it would have chosen in the absence of cascading. For each existing cascade-for-size conference on an MCU, it subtracts the number of video ports reserved for cascading from the number of video ports available when calculating port availability.

Cascading for size may not be appropriate for all conferences and should be used selectively. In addition to possible transmission delays, each cascade-for-size conference reserves ports on the MCU, reducing the ports available for participants. Enabling cascading for size for conferences that don’t require cascading underutilizes MCU resources.

When a conference is cascaded across multiple MCUs, the video and audio from each MCU is transmitted to every other MCU through cascade links. This incurs some delay. In a conference with many cascade links, this delay may become noticeable to the participants. The transmission delay isn't noticeable in one-way communication or when all the speakers are on the same MCU. For this reason, large cascaded conferences are best suited to presentation-style conferences where only a few participants on the same MCU speak, and other participants only listen.

You can enable cascade-for-size conferences with these steps:

- Enable cascading for size in some or all of your conference templates.
- For one or more of your MCUs, specify the number of ports per cascade-for-size conference to reserve for cascade links.
Processing a Cascaded-for-Size Call

Once a conference with cascading for size enabled has started (the “hub” MCU), the RealPresence DMA system completes the following process for each subsequent participant that dials into that conference:

- From among the MCUs that are currently part of the conference and have ports available that are not reserved for cascading, the RealPresence DMA system randomly selects one of the MCUs closest to the hub MCU, or the hub MCU itself.

- If on every MCU that is currently part of the conference, all available ports are reserved for cascading, the RealPresence DMA system does the following:
  - From among the MCUs that are currently part of the conference and that have ports available for the cascade link, the RealPresence DMA system selects the one closest to the hub MCU, or the hub MCU itself.
  - It selects a new MCU to join the conference, using the same selection process used for selecting the first (hub) MCU, and creates the cascade link to it.
  - If no MCU has ports available for cascade links, the RealPresence DMA system rejects the call.
WebRTC Conferencing

Topics:

- WebRTC Conference Templates

WebRTC participants start or enter a conference by connecting to the Polycom RealPresence Web Suite Experience Portal, which manages signaling between WebRTC clients and the RealPresence DMA system.

The RealPresence DMA system can’t accept WebRTC calls directly from a WebRTC client.

Small conferences including up to three WebRTC participants don’t require an MCU. This is known as mesh conferencing mode. In this mode, the WebRTC media streams are passed directly from client to client.

In certain conferencing situations, a mesh conference must be escalated to an MCU. When required, the RealPresence DMA system assigns a WebRTC-capable MCU to host the conference:

- If a fourth participant joins the conference.
- If a non-WebRTC participant joins the conference.
- If certain conference features are needed, such as conference recording.

Once an MCU is assigned to host the conference, participants using WebRTC clients have the same experience as participants using SIP or H.323 endpoints. If a WebRTC client dials a conference that requires an MCU and the system selects an MCU that doesn’t support WebRTC, the client is disconnected. For this reason, Polycom recommends creating MCU pool orders that consist only of MCUs that support WebRTC.

The following limitations apply to WebRTC conferencing:

- WebRTC participants cannot enter conferences by dialing VEQs.
- WebRTC conferences don’t support the SVC only conference mode.
- Some conference template settings are not compatible with the WebRTC with mesh only or WebRTC with MCUs or mesh settings.
- WebRTC with mesh only conference templates are not supported for Polycom RealConnect conferences.
- Cisco Codian options are disabled when you enable WebRTC conferencing.

WebRTC Conference Templates

Some conference template settings are incompatible with WebRTC conferences.

If you enable WebRTC with mesh only in a conference template and select incompatible settings, the system displays an error about the incompatibilities when you click OK in the Add Conference Template window. You can use this information to disable the incompatible features, or close the conference template dialog and begin again.

If a conference uses a template with the WebRTC with MCUs or mesh setting enabled, requesting a conference feature that is incompatible with mesh mode during a conference causes the system to promote the conference to an MCU. This allows the participant to use the requested feature, and the conference proceeds normally.
The following conference template settings are compatible with conferences in mesh mode. If you enable settings not in this list for a mesh-only conference, the RealPresence DMA system will display an error.

- **Polycom MCU General Settings**
  - Line rate
  - Encryption
  - Enable FECC
  - FW NAT keep alive
  - FW NAT keep alive interval (seconds)
- **Polycom MCU Video Quality**
  - Multiple content resolutions
- **Polycom MCU Video Settings**
  - Lecturer view switching
- **Polycom MCU Audio Settings**
  - Mute participants except lecturer
  - NoiseBlock (MPMx or newer)
  - Speaker change threshold (MPMx or newer)
- **Polycom MCU Site Names** (all settings)
About Conference IVR Services

In a template, you can optionally specify the conference interactive voice response (IVR) service that the Polycom MCU should use.

However, this is not recommended. Polycom MCUs have two defaults, one for conferences with passcodes and one for conferences without passcodes. For conferences configured via the RealPresence DMA system, which are not linked to a profile, the MCU automatically uses the correct default IVR service for each conference.

If you choose to override the default and specify an IVR service, the IVR service you select must be appropriate for the users whose conferences will use this template, and it must be available on the MCUs on which those conferences may take place. See your Polycom MCU documentation for information about conference IVR services. This feature is not supported on Cisco Codian MCUs.

When you add or edit a conference template, the Polycom MCU Conference IVR tab contains a list of all the conference IVR services available on the currently connected MCUs. Note that when you add an MCU, its conference IVR services won't immediately display in the list and you must close and reopen the add or edit a conference template window to refresh the list. If an IVR service is only available on some of the connected MCUs, its entry shows how many of the MCUs have that IVR service.

If a template specifies a conference IVR service, the system will put conferences using that template on the least used MCU that has that conference IVR service. If there are none, it falls back to the default conference IVR service.

Callers to conferences with passcodes (PINs) can bypass the IVR service's passcode prompting by appending the passcode to the dial string, following the protocol-appropriate delimiter:

- H.323 - <vmr number>#$<passcode>
- SIP - <vmr number>**<passcode>
IVR Prompt Sets

Topics:

- View an IVR Prompt Set
- Add a Custom IVR Prompt Set

A prompt set contains a set of media files (audio prompts and video slides) that provide the caller experience for a RealPresence DMA -controlled IVR service.

The RealPresence DMA system comes with a factory default call flow and corresponding prompt set. You can customize the IVR experience, in terms of language or branding, associated with the call flow by installing custom prompt sets and creating RealPresence DMA -controlled VEQs that use those prompt sets.

A prompt set is an archive (.zip) file containing:

- A directory, META-INF, containing a single file, MANIFEST.MF. This is a text file describing the prompt set. It contains name:value attribute pairs separated by newlines. Currently, the RealPresence DMA system checks the following attribute names for valid values:
  - **AppName** identifies the call flow associated with this prompt set. Currently, dma7000 is the only valid value.
  - **Promptset** is the name of the prompt set. This value must be unique across all prompt set zip files.

  The following example is a valid custom manifest file (note that a custom manifest file requires two carriage returns at the end of the file):

  ```
  Manifest-Version: 1.0
  Ant-Version: Apache Ant 1.9.3
  Created-By: 1.6.0_21-b07 (Sun Microsystems Inc.)
  AppName: dma7000
  Promptset: custompromptset
  
  Note: The manifest file must not contain the attribute names Format and Language.
  ```

- A collection of .wav and .jpg files with the individual audio prompts and video slides.

  The .wav files should be encoded in PCM 16 kHz 16-bit mono format, and the file names must be exactly the same as in the default prompt set. If a custom prompt set is missing the .wav file for a specific prompt in the call flow, the RealPresence DMA system substitutes the corresponding prompt from the factory default prompt set.

  The .jpg files should be 1920x1088 pixels, and the file names must be exactly the same as in the default prompt set. If a custom prompt set is missing a .jpg file, the RealPresence DMA system substitutes the corresponding one from the factory default prompt set.

  **Note:** The RealPresence DMA system doesn't examine the contents of the media files to validate the format.

The call flow currently uses only one video slide, General_Slide.jpg. The following table lists the audio prompt files it uses.
<table>
<thead>
<tr>
<th>Prompt File Name</th>
<th>Prompt Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson_Identifier.wav</td>
<td>For conference chairperson services, enter the chairperson password. All other participants, please wait.</td>
</tr>
<tr>
<td>Chairperson_PIN_Invalid.wav</td>
<td>Invalid chairperson password.</td>
</tr>
<tr>
<td>Chairperson_PIN_Invalid_Retry.wav</td>
<td>Invalid chairperson password. Please try again.</td>
</tr>
<tr>
<td>Conference_Full.wav</td>
<td>The conference is full. You cannot join at this time.</td>
</tr>
<tr>
<td>Conference_Locked.wav</td>
<td>The conference is locked. You cannot join at this time.</td>
</tr>
<tr>
<td>Conference_NID.wav</td>
<td>Please enter the conference ID.</td>
</tr>
<tr>
<td>Conference_NID_Invalid.wav</td>
<td>Invalid conference ID.</td>
</tr>
<tr>
<td>Conference_NID_Invalid_Retry.wav</td>
<td>Invalid conference ID. Please try again.</td>
</tr>
<tr>
<td>Conference_PIN.wav</td>
<td>Please enter the conference password.</td>
</tr>
<tr>
<td>Conference_PIN_Invalid.wav</td>
<td>Invalid conference password.</td>
</tr>
<tr>
<td>Conference_PIN_Invalid_Retry.wav</td>
<td>Invalid conference password. Please try again.</td>
</tr>
<tr>
<td>Disconnect.wav</td>
<td>You'll now be disconnected.</td>
</tr>
<tr>
<td>General_Welcome.wav</td>
<td>Welcome to unified conferencing.</td>
</tr>
<tr>
<td>No_Resources_Available.wav</td>
<td>Sorry, the system is full.</td>
</tr>
<tr>
<td>Operator_Transfer.wav</td>
<td>You'll now be transferred to the operator.</td>
</tr>
<tr>
<td>Operator_Transfer_Cancelable.wav</td>
<td>Press any key to cancel.</td>
</tr>
</tbody>
</table>

**View an IVR Prompt Set**

You can view current IVR prompt sets and details about the included prompts.

**Procedure**

1. Go to **Service Config > Conference Manager Settings > IVR Prompt Sets**. The list of current IVR prompt sets displays.
2. Select an IVR prompt set to view detailed information about the included prompts. The **Prompt Set Details** pane displays information about the selected IVR prompt set.
### Add a Custom IVR Prompt Set

You can add a custom interactive voice response (IVR) prompt set and associate it with a Virtual Entry Queue.

**Procedure**

2. Go to [Service Config > Conference Manager Settings > IVR Prompt Sets](#).
3. Under **Actions**, click **Add IVR Prompt Set Archive**.
4. Navigate to the file you want to use and click **Open**.

The system validates the **Appname** and **Promptset** values in the manifest file of the prompt set archive.
Shared Number Dialing

Topics:

- Shared Number Dialing Call Flow
- Virtual Entry Queues
- Add a Virtual Entry Queue
- Add a Direct Dial Virtual Entry Queue
- Edit a Virtual Entry Queue
- Edit a Direct Dial Virtual Entry Queue
- Test Script Debugging for VEQ Scripts
- Sample Virtual Entry Queue Script

The RealPresence DMA system can be configured to handle SIP calls to certain shared numbers (virtual entry queues) by routing them to an appropriate Polycom MCU entry queue.

Depending on the MCU type and version, Polycom MCUs can have two kinds of entry queues for providing callers with interactive voice response (IVR) services:

- **MCU-controlled entry queues** - The prompts, slides, and call flow providing the IVR experience reside on the MCU. Polycom MCUs refer to these as **IVR-only service provider entry queues**.

- **RealPresence DMA-controlled entry queues** (referred to as **External IVR control entry queues** on supporting MCUs because the IVR control is external to the MCU) - The prompts, slides, and call flow providing the IVR experience reside on the RealPresence DMA system (see **IVR Prompt Sets**).

A virtual entry queue (VEQ) connected to either type of MCU entry queue enables you to publicize a shared number that can be used to reach multiple virtual meeting rooms (VMRs), local RealConnect conferences, or RealConnect conferences hosted on external Skype for Business systems. When a caller dials the shared number, the RealPresence DMA system routes the call to an MCU with the resources and capability to provide the IVR experience associated with the shared number.

Related Links

- Add a Standalone Conference Template on page 251
- Add a Linked Conference Template on page 266
- Edit a Conference Template on page 267
- Delete a Conference Template on page 267
- Select a Video Frames Layout
- Alert 6002 on page 594

**Shared Number Dialing Call Flow**

For RealPresence DMA-controlled VEQ numbers, the RealPresence DMA system recognizes two speed dial SIP dial string formats:
- `<veq number>**<conference ID>` - The system validates the conference ID. If it's valid, the caller bypasses the prompt for the destination conference. If the VMR has a conference passcode (PIN), chairperson passcode, or both, the system prompts for and validates the passcode.

- `<veq number>**<conference ID>**<passcode>` - The system validates the conference ID, and if it's valid, the passcode. If both are valid, the caller bypasses both prompts and is placed directly into conference.

The RealPresence DMA system processes the shared number dialing call flow as follows:

1. Callers dial a shared number to reach the RealPresence DMA system.

2. The RealPresence DMA system recognizes the dialed number as a VEQ number and routes the call to a Polycom MCU configured to provide the IVR experience (MCU-controlled or RealPresence DMA- controlled) that's associated with the VEQ number dialed.

3. If this is an MCU-controlled entry queue:
   a. The MCU uses its call flow, voice prompts, and video slides, to prompt the caller for the conference ID of the destination conference and sends the response back to the RealPresence DMA system for validation.
   b. The RealPresence DMA system validates the conference ID entered by the caller. If the number is invalid, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable.
   c. If the caller entered a valid conference ID, the RealPresence DMA system routes the call to the conference (selecting an appropriate MCU and starting the conference if necessary). Prompting for a passcode, if needed, is handled by the conference IVR service assigned to the conference template, if any, or the default conference IVR service.

4. If this is a RealPresence DMA-controlled entry queue:
   a. The RealPresence DMA system uses its call flow, voice prompts, and video slides, to send commands to the MCU to control the interaction with the caller (display slides, play prompts, collect tones, etc.).
   b. The RealPresence DMA system validates the conference ID entered by the caller. If the caller entered an invalid number, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable. If the caller fails to enter a valid number or enters the (configurable) operator request command, the RealPresence DMA system routes the call to the operator (help desk) SIP URI.
   c. If the conference has a conference passcode (PIN), chairperson passcode, or both, the RealPresence DMA system instructs the MCU to prompt for and collect the passcode. The RealPresence DMA system validates the passcode entered by the caller. If the caller entered an invalid passcode, the RealPresence DMA system instructs the MCU to re-prompt the caller. The number of retries is configurable. If the caller fails to enter a valid passcode or enters the (configurable) operator request command, the RealPresence DMA system routes the call to the operator (help desk) SIP URI.
   d. If the caller entered a valid passcode, the RealPresence DMA system routes the call to the conference (selecting an appropriate MCU and starting the conference if necessary), assigning the caller the appropriate role (chairperson or participant).
Virtual Entry Queues

The default dial plans contain a dial rule that routes calls whose dialed number is a VEQ dial-in number to the correct VEQ.

You can create up to 60 different VEQs to provide different IVR experiences (for example, different language prompts or different greetings). You can designate one of the MCU-controlled VEQs as the Direct Dial VEQ, and the system will use it for calls dialed without a VEQ or conference ID. For instance, if a call's dial string includes only the system's domain name or IP address, the RealPresence DMA system uses the Direct Dial VEQ for it.

For MCU-controlled VEQs, to create a unique experience, you must create the corresponding entry queue on the Polycom MCUs to be used.

For RealPresence DMA-controlled VEQs, the MCU's entry queue must be one of its External IVR Entry Queues. The prompt set for the VEQ must be installed on the RealPresence DMA system. Different External IVR Entry Queues can be created on the MCUs to provide different profiles (bit rate, resolution, etc.) for the pre-conference phase, but most of the entry queue experience (language, prompts, retries, and timers) is defined by the RealPresence DMA-controlled VEQ.

View Virtual Entry Queues

You can view existing virtual entry queues (VEQs).

The Shared Number Dialing page lists the VEQs available on the system and enables you to add, edit and delete VEQs.

The entry queues created for shared number dialing VEQs must have the IVR only service provider setting selected. See your Polycom MCU documentation.

When selecting an MCU to handle IVR for a VEQ, the RealPresence DMA system chooses from among MCUs that have the entry queue specified for that VEQ, without regard to MCU pool orders.

Ensure that the entry queue is available on the MCUs to be used and that it's the same on each MCU.

Procedure

» Go to Service Config > Conference Manager Settings > Shared Number Dialing.

The following table describes the fields on the page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual entry queue</td>
<td>The VEQ number. For example 12345, or Direct Dial.</td>
</tr>
<tr>
<td>Dial-in #</td>
<td>The complete dial string, for this VEQ. For example, if the system uses the prefix 71, this might be 7112345.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The name of the Polycom MCU entry queue (IVR experience) to be used for callers to this VEQ.</td>
</tr>
</tbody>
</table>
Add a Virtual Entry Queue

You can add a virtual entry queue (VEQ) to the list of configured VEQs.

Procedure

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Under Actions, click Add Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Entry Queue</td>
<td></td>
</tr>
<tr>
<td>Virtual entry queue number</td>
<td>The VEQ number.</td>
</tr>
<tr>
<td>Dial-in number</td>
<td>Number used to dial into the VEQ.</td>
</tr>
<tr>
<td></td>
<td>This is automatically set to the dialing prefix in Conference Settings,</td>
</tr>
<tr>
<td></td>
<td>plus VEQ number.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for this VEQ and its IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ.</td>
</tr>
<tr>
<td></td>
<td>The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
</tbody>
</table>

**Note:** Polycom MCUs refer to entry queues designed for a RealPresence DMA -controlled VEQ as External IVR because RealPresence DMA -based IVR control is external to the MCU.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system. If enabled, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system doesn’t exist in the dial rule’s Selected external Skype systems box, the dial rule fails and the next dial rule is tried. If not enabled, the system attempts to match the incoming DTMF against all defined external Skype for Business systems.</td>
</tr>
</tbody>
</table>

**DMA-based IVR Call Flow (only for External IVR control entry queues)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Valid DTMF responses to conference ID prompt | The values a caller can enter when responding to a prompt for a conference ID:  
  Conference room ID (VMR)  
  Conference room alias  
  RealConnect conference ID |
| IVR prompt set | The prompt set to be used for a RealPresence DMA-controlled VEQ. The list includes all those installed on the RealPresence DMA system. |
| Timeout for response entry (sec) | The length of time that the RealPresence DMA system waits for a caller to respond to a prompt (5-60 seconds). |
| DTMF terminator | The terminator used to mark the end of caller input. |
| Operator assistance URI | The SIP URI to which to route the call for operator (help desk) assistance. |
| Request operator transfer DTMF | The DTMF command for requesting an operator.  
  **Note:** If this digit string matches a VMR number, that VMR becomes unreachable. |
| Timeout to cancel operator request (sec) | The length of time after requesting an operator that a caller is given to cancel that request (1-10 seconds).  
  **Note:** An operator request can be canceled by entering any DTMF key. |
| Script | Scripts entered in this section have access to the DTMF digits entered by callers. The system executes these scripts during VEQ processing, and can change and reject the DTMF digits callers enter. You can use this functionality to strip prefixes entered by a caller or to authorize participants dialing in to VEQs. These scripts are written in the JavaScript language. |
| Enabled | Enable or disable the script in the Script text box. |
| Script | Type (or paste) the VEQ script you want to apply. Then click **Debug this Script** to test the script with various variables. |
4. Click OK.

Related Links
Sample Virtual Entry Queue Script on page 287

Add a Direct Dial Virtual Entry Queue

You can add a direct dial virtual entry queue (VEQ) to the list of configured VEQs.

Procedure
1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. In the Actions pane, click Add Direct Dial Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description for this VEQ and its IVR experience, for example: Direct Dial - English.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system. If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems. If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system doesn’t exist in the dial rule’s Selected external Skype systems box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>

4. Click OK.

Edit a Virtual Entry Queue

You can edit a virtual entry queue (VEQ) as needed.

Procedure
1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Select the virtual entry queue of interest and click Edit Virtual Entry Queue.
3. Revise the following fields as needed:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Entry Queue</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual entry queue number</td>
<td>The VEQ number.</td>
</tr>
<tr>
<td>Dial-in number</td>
<td>Number used to dial into the VEQ. Automatically set to the dialing prefix in Conference Settings, plus VEQ number.</td>
</tr>
<tr>
<td>Description</td>
<td>A meaningful description for this VEQ and its IVR experience, such as which language is used.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Polycom MCUs refer to entry queues designed for a RealPresence DMA -controlled VEQ as External IVR because RealPresence DMA -based IVR control is external to the MCU.</td>
</tr>
<tr>
<td>Unique external Skype system</td>
<td>Instructs the system to attempt to resolve DTMF as a Skype conference ID for a specific external Skype for Business system.</td>
</tr>
<tr>
<td></td>
<td>If this option is off, the system attempts to match the incoming DTMF against all defined external Skype for Business systems.</td>
</tr>
<tr>
<td></td>
<td>If this option is on, the system attempts to match the incoming DTMF against the specific external Skype for Business system you choose from the list. If a match is found, the appropriate dial rule is executed. If the selected unique external Skype for Business system doesn’t exist in the dial rule’s <strong>Selected external Skype systems</strong> box, the dial rule fails and the next dial rule is tried.</td>
</tr>
</tbody>
</table>

**DMA-based IVR Call Flow (only for External IVR control entry queues)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DTMF responses to conference ID prompt</td>
<td>The values a caller can enter when responding to a prompt for a conference ID:</td>
</tr>
<tr>
<td></td>
<td><strong>Conference room ID (VMR)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Conference room alias</strong></td>
</tr>
<tr>
<td></td>
<td><strong>RealConnect conference ID</strong></td>
</tr>
<tr>
<td>IVR prompt set</td>
<td>For a RealPresence DMA -controlled VEQ, the prompt set to be used. The list includes all those installed on the RealPresence DMA system.</td>
</tr>
<tr>
<td>Timeout for response entry (sec)</td>
<td>The length of time that the RealPresence DMA system waits for a caller to respond to a prompt (5-60 seconds).</td>
</tr>
<tr>
<td>DTMF terminator</td>
<td>The terminator used to mark the end of caller input.</td>
</tr>
<tr>
<td>Operator assistance URI</td>
<td>The SIP URI to which to route the call for operator (help desk) assistance.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Request operator transfer DTMF | The DTMF command for requesting an operator. **Note:** If this digit string matches a VMR number, that VMR becomes unreachable.

Timeout to cancel operator request (sec) | The length of time after requesting an operator that a caller is given to cancel that request (1-10 seconds). **Note:** An operator request can be canceled by entering any DTMF key.

Script | Scripts entered in this section have access to the DTMF digits entered by callers. The system executes these scripts during VEQ processing, and can change and reject the DTMF digits callers enter. You can use this functionality to strip prefixes entered by a caller or to authorize participants dialing in to VEQs. These scripts are written in the Javascript language.

Enabled | Enable or disable the script in the Script text box.

Script | Type (or paste) the VEQ script you want to apply. Then click Debug this Script to test the script with various variables.

4. Click OK.

**Related Links**
- [Sample Virtual Entry Queue Script](#) on page 287

## Edit a Direct Dial Virtual Entry Queue

You can edit a direct dial virtual entry queue (VEQ) when necessary.

**Procedure**

1. Go to Service Config > Conference Manager Settings > Shared Number Dialing.
2. Select the direct dial virtual entry queue you’d like to edit and click Edit Direct Dial Virtual Entry Queue.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A meaningful description for this VEQ and its IVR experience, for example: Direct Dial – English.</td>
</tr>
<tr>
<td>Response entry attempts</td>
<td>The number of times a caller can enter an invalid VMR number before the system rejects the call.</td>
</tr>
<tr>
<td>Polycom MCU entry queue</td>
<td>The Polycom MCU entry queue to use for this VEQ. The list includes all entry queues available on the Polycom MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.</td>
</tr>
</tbody>
</table>
### Test Script Debugging for VEQ Scripts

You can test a JavaScript executable script that you've associated with a virtual entry queue (VEQ). It lets you specify parameters of a call and the DTMF string entered by a caller, observing the result of the script.

**Procedure**

1. Navigate to **Service Config > Conference Manager Settings > Shared Number Dialing**.
2. In the **Actions** pane, click **Edit Virtual Entry Queue**.
3. In the **Edit Virtual Entry Queue** dialog, select **Scripts**.

The following table describes the fields in the dialog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dial string</strong></td>
<td>The <code>DIAL_STRING</code> variable in the script. Enter a dial string if script execution depends on this variable. Alternatively, provide the entire <code>SIP INVITE</code> message. <strong>Note</strong>: For SIP, the script should always specify the schema prefix (sip or sips). For example:</td>
</tr>
<tr>
<td></td>
<td><code>DIAL_STRING = &quot;sip:xxx@10.33.120.58&quot;</code></td>
</tr>
<tr>
<td><strong>DTMF digits</strong></td>
<td>Enter the DTMF digits, corresponding to the script variable <code>DTMF_STRING</code>, that should be evaluated or transformed by the script.</td>
</tr>
<tr>
<td><strong>Caller site</strong></td>
<td>Select a site in order to set the first four caller variables.</td>
</tr>
<tr>
<td><strong>Caller variables</strong></td>
<td>Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Final result</td>
<td>Displays the outcome of running the script. If the script rejected the DTMF string, a message tells you so. Otherwise, the transformed DTMF string is displayed.</td>
</tr>
<tr>
<td>Script output</td>
<td>Displays any output produced by the script (for example: println statements).</td>
</tr>
<tr>
<td>Output SIP headers</td>
<td>Displays any SIP headers produced by the script.</td>
</tr>
</tbody>
</table>

4. Complete the required fields and click **Debug this Script**.

**Sample Virtual Entry Queue Script**

Virtual entry queue (VEQ) scripts are written in the JavaScript language that have access to the DTMF digits entered by callers.

The system executes these scripts during VEQ processing, and can change and reject the DTMF digits callers enter. You can use this functionality to strip prefixes entered by a caller or to authorize participants dialing in to VEQs.

VEQ scripts have access to the `DTMF_STRING` variable.

You can use `return ACCEPT;` and `return REJECT;` statements to accept or reject the entered DTMF digits. When you `return ACCEPT`, the script accepts the entered DTMF digits as is. When you `return REJECT`, the system doesn't accept the DTMF digits and prompts the caller again for new DTMF input.

The following sample script shows how to use the scripting feature to restrict participants calling a specific VEQ to a whitelist of VMRs.

```javascript
var whitelist_vmrs = [
  "1000",    // Specify list of VMRs; add or remove VMRs from this list.
  "2000",    // Make sure you use the syntax "<vmr number>"<comma>
  "3000",
];
var whitelist_patterns = [
  "^44",    // The ^ causes the pattern match at the beginning of the string.
  "^76"     // So 441000 will match but 100044 will not.
];

// Match against individual VMRs. ACCEPT if any of them matches.
// if (0 <= whitelist_vmrs.indexOf(DTMF_STRING))
//  return ACCEPT;
//
// Match against patterns. ACCEPT if any of them matches.
//
```
for (i=0; i<whitelist_patterns.length; i++)
{
    if (DTMF_STRING.match(whitelist_patterns[i]))
    {
        return ACCEPT;
    }
    return REJECT;

Related Links
Add a Virtual Entry Queue on page 281
Edit a Virtual Entry Queue on page 283
SIP Conference Factories

Topics:

- Working with SIP Conference Factories

SIP conference factories enable users on some brands and models of endpoints to escalate a point-to-point call to an ad hoc, multiparty conference call on a Polycom MCU.

SIP conference factories create conferences based on a dial rule with the action to resolve to a SIP conference factory.

Working with SIP Conference Factories

Users with certain brands and models of endpoints (known as escalating endpoints) can escalate multiple point-to-point calls to a RealPresence DMA conference by calling a SIP conference factory.

When the RealPresence DMA system receives an incoming call from an escalating endpoint to a SIP conference factory, the system creates a dynamic multi-point conference on an MCU and generates a conference ID for the conference. The conference IDs are strings that can be dialed by any endpoint (SIP or H.323) to join the conference. These conference IDs are not VMR IDs and the conferences do not have associated VMRs.

Once the RealPresence DMA system creates the dynamic conference, the escalating endpoint invites itself to the conference and then transfers (refers) its calls with other endpoints into the multi-point conference. Any user attending the conference can then invite other participants by providing them with the conference ID.

Note: Unlike VMR conferences, SIP conference factory conferences are not associated with individual RealPresence DMA users and are not included in VMR queries. SIP conference factory conferences are resolvable by the test dial rules feature.

The RealPresence DMA system provides a pre-configured SIP conference factory with the SIP conference factory ID `plcm-scf`. You can edit this SIP conference factory as needed or delete it. This default SIP conference factory creates conferences using the default conference template, the default MCU pool order, in the default territory within the system’s site topology.

The RealPresence DMA system default dial plan includes the dial rule `Dial to SIP conference factory` that you can enable to support SIP conference factories.

Any number of dial rules with the action to `Resolve to SIP conference factory` may be included in a dial plan.

Add a SIP Conference Factory

You can add SIP conference factories in the RealPresence DMA system to support escalation of point-to-point calls to multi-point calls.

Procedure

1. Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2. Click the Add button.
3. Complete the fields described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference factory ID*</td>
<td>The unique ID of the SIP conference factory. This is the dial string that invokes the SIP conference factory. Conference Factory IDs must meet the following requirements in order to be valid: • Must start and end with an alphanumeric character. • Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ &amp; , . ' = + - * ( ) • % is allowed only if it's followed by at least three alphanumeric characters. • Cannot contain blank spaces.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the SIP conference factory.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The conference template that defines the properties of a SIP conference factory conference. Defaults to the conference template configured in Conference Settings.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order that specifies the order in which the MCU pools are used. Defaults to the MCU pool order configured in Conference Settings.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory assigned to a SIP conference factory conference room if it isn't specified at the conference room level.</td>
</tr>
</tbody>
</table>

4. Click OK.

**Edit a SIP Conference Factory**

You can edit SIP conference factory settings as needed in the RealPresence DMA system to support escalation of point-to-point calls to multi-point calls.

You can also disable a SIP conference factory without deleting it.

**Procedure**

1. Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2. Select the SIP conference factory to revise and click the Edit button.
3. Revise the fields described in the following table as needed.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Conference factory ID* | The unique ID of the SIP conference factory. This is the dial string that invokes the SIP conference factory. Conference Factory IDs must meet the following requirements in order to be valid:  
  - Must start and end with an alphanumeric character.  
  - Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ & , . ' = + - * ( )  
  - % is allowed only if it’s followed by at least three alphanumeric characters.  
  - Cannot contain blank spaces. |
| Description           | A brief description of the SIP conference factory.                                                                                         |
| Conference template   | The conference template that defines the properties of a SIP conference factory conference. Defaults to the conference template configured in Conference Settings. |
| MCU pool order        | The MCU pool order that specifies the order in which the MCU pools are used. Defaults to the MCU pool order configured in Conference Settings.       |
| Territory             | The territory assigned to a SIP conference factory conference room if it isn’t specified at the conference room level.                         |

4. Click OK.

**Disable a SIP Conference Factory**

When you add a new SIP conference factory, it’s enabled by default. You can disable the SIP conference factory if necessary without deleting it.

**Procedure**

1. Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2. Select the SIP conference factory to disable and click the Disable button.
   
   The SIP conference factory is disabled but is not deleted.

**Enable a SIP Conference Factory**

If you’ve previously disabled a SIP conference factory, you can enable it again when necessary.

**Procedure**

1. Go to Conference Manager Settings > SIP Conference Factories.
2. Select the SIP conference factory to enable and click the Enable button.
   
   The SIP conference factory is enabled.
Delete a SIP Conference Factory
You can delete a SIP conference factory if it will no longer be used.

Procedure
1. Go to Service Config > Conference Manager Settings > SIP Conference Factories.
2. Select the SIP conference factory to delete and click Delete.
3. Click Yes to confirm the deletion.
Presence Publishing for Skype

Topics:

- Configure Presence Publishing for Skype

The RealPresence DMA system can be integrated with Microsoft Skype for Business environments. When you integrate the RealPresence DMA system with a Skype environment, the system communicates with the Skype servers and Active Directory to provide contact presence and conference interaction between MCUs managed by the RealPresence DMA system and the Skype AVMCU. Contact presence allows Skype clients to view the presence of a RealPresence DMA system VMR, similar to any other contact in the Skype client contact list.

Configure Presence Publishing for Skype

If your RealPresence DMA system is integrated with a Microsoft Skype for Business environment, you can configure default presence publishing settings for Polycom conference contacts.

Before you configure presence publishing, confirm that your RealPresence DMA system's identity certificate contains accurate information. An incorrect certificate may cause an error when the RealPresence DMA system attempts to contact the Skype for Business server to update the presence status.

Procedure

2. Complete the fields described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish presence for Polycom conference contacts</td>
<td>When checked, presence status for each conference contact is visible in the Skype for Business contact window.</td>
</tr>
<tr>
<td>Skype pool to create/publish to</td>
<td>A list of Microsoft SIP peer pools to which the RealPresence DMA system can publish presence. Select the pool whose clients should see presence indications for conference contacts. A Skype pool will appear in the list if:</td>
</tr>
<tr>
<td></td>
<td>- The pool is defined as an External SIP Peer with Microsoft selected as the Type.</td>
</tr>
<tr>
<td></td>
<td>- The field Maximum Polycom conference contacts to publish in the External SIP Peer Skype Integration tab is set to a value greater than zero.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Contact SIP domain</td>
<td>The domain portion of the SIP URI that the RealPresence DMA system uses for a conference contact (for example, sipdomain.net). The conference contacts are created in this domain. If the domain doesn’t exist, it will be created if the <strong>Create Polycom conference contacts</strong> check box is enabled. If multiple superclusters are integrated with a Skype for Business environment, this field should be different for each supercluster. If this value is the same across multiple superclusters and the systems are integrated with the same Active Directory, settings changes on one supercluster could affect other superclusters. When you enable the <strong>Publish presence for Polycom conference contacts</strong> check box and <strong>Update</strong> the settings, a warning may display.</td>
</tr>
<tr>
<td>Create Polycom conference contacts</td>
<td>Only available if Microsoft Active Directory integration is enabled. When checked, the RealPresence DMA system will create Active Directory resources for any meeting rooms that have the <strong>Presence</strong> option enabled. If you haven’t changed the <strong>Presence</strong> option manually for any VMRs, all VMRs will have corresponding Active Directory contacts created.</td>
</tr>
<tr>
<td>VMR display name pattern</td>
<td>The text pattern that describes the name of the VMR contact. This text will precede the VMR number when displayed in the Skype contact window (for example, a VMR display name pattern of Conference room would create display names of Conference room &lt;VMR number&gt;). The maximum pattern length is 63 characters. After you edit this field, it may take some time for the change to be seen in the Skype client, depending on how many conference contacts the RealPresence DMA system is managing.</td>
</tr>
<tr>
<td>OU for contacts</td>
<td>The Active Directory OU (Organizational Unit) in which the RealPresence DMA system should create contact resources. If left blank, the system creates resources in the CN=Users container.</td>
</tr>
<tr>
<td>Default Polycom conference contacts presence settings</td>
<td>Changes the default system-wide setting for VMR presence publishing and Active Directory contact creation. The setting in this field can be overridden by the <strong>Presence</strong> setting for a user’s conference room.</td>
</tr>
</tbody>
</table>

3. Select the **Default Polycom conference contacts presence settings** as follows:
   - If the **Publish presence for Polycom conference contacts** option is checked and the **Create Polycom conference contacts** is unchecked, choose one of the following settings:
     - **Publish Polycom conference contacts presence**
     - **Do not publish Polycom conference contacts presence**
   - If both the **Publish presence for Polycom conference contacts** option and the **Create Polycom conference contacts** option are checked, choose one of the following settings:
     - **Create Polycom conference contacts and publish presence**
     - **Do not create Polycom conference contacts or publish presence**
4. Click Update to save the settings.

Remove Contacts from Active Directory

If you disable the Publish presence for Polycom conference contacts option and Active Directory integration is enabled, the Remove Contacts from Active Directory action becomes available in the left-hand navigation pane.

For systems integrated with a Microsoft Skype for Business environment, this action allows you to remove any contacts in Active Directory created by the RealPresence DMA system.

Removing contacts will apply to contacts created by any supercluster integrated with the Active Directory.

If you remove all contacts across all SIP domains, the conference contacts associated with other RealPresence DMA system superclusters that were removed will be automatically recreated daily when the systems sync with Active Directory. You can also manually recreate these contact resources.

Procedure

2. Uncheck Publish presence for Polycom conference contacts.
3. Click Update.
4. Click Remove Contacts from Active Directory and choose one of the following options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove all Polycom conference contacts associated with contact SIP domain</td>
<td>Limit the change to one SIP domain. The default value in the text field is the current SIP domain in the Contact SIP domain field.</td>
</tr>
<tr>
<td>Remove all Polycom conference contacts associated with any contact SIP domain</td>
<td>All conference contacts created by the RealPresence DMA system are removed, regardless of SIP domain.</td>
</tr>
</tbody>
</table>

5. Click Update.

Recreate Skype Contact Resources

You can manually recreate Microsoft Skype for Business contact resources associated with other superclusters.

Procedure

1. Log in to a system on one of the affected superclusters.
2. Go to Service Config > Conference Manager Settings > Presence Publishing for Skype.
3. Uncheck Publish presence for Polycom conference contacts.
4. Click Update.
5. Select Publish presence for Polycom conference contacts.
6. Click Update.
   A caution dialog may appear regarding contact SIP domains for multiple superclusters.
7. Click OK.
8. Repeat the preceding steps for any other affected superclusters.
Call Server Configuration

Topics:

- Call Server Settings
- Dial Plans
- Prefix Service
- Hunt Groups
- Domains Restrictions
- Preliminary and Postliminary Scripting

This section provides an introduction to configuring the RealPresence DMA system’s call server.
Call Server Settings

Topics:

- Configure the Call Server

The RealPresence DMA system's call server capabilities can provide gatekeeper functionality, SIP proxy server and registrar functionality, bandwidth management, and registration sharing from an edge-configured system to a core-configured system.

The call server can also function as an H.323-to-SIP and SIP-to-H.323 gateway. The gateway function is used only for calls to registered endpoints, SIP peers, and H.323 gatekeepers. It is not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), or external IP addresses and doesn't support content sharing or AES encryption.

The call server also supports SIP forking, where multiple SIP devices may be dialed simultaneously. The first callee to answer gets the call and the remaining callees are gracefully disconnected. The RealPresence DMA system will initiate SIP forking in the following situations:

- More than one SIP endpoint contact address is registered to the RealPresence DMA system with the same address-of-record (AOR), another endpoint dials to the system using that same AOR, and the **Dial by Registered Endpoint** dial action resolves this dial attempt.
- Multiple SIP peers are configured for a **Dial by SIP Peer** dial rule action, and that action is used to resolve a dial attempt to the RealPresence DMA system.

Related Links

- Add a Site on page 422
- View the Site Information on page 421
- Edit a Site on page 428
- Add a Subnet on page 433
- Edit a Subnet on page 434
- Add a Site Link on page 436
- Edit a Site Link on page 437

Configure the Call Server

You can specify the general, gatekeeper, and SIP proxy settings that the call server uses.

These settings apply to all RealPresence DMA systems in a supercluster.

Procedure

1. Go to **Service Config > Call Server Settings**.
2. Configure the call server settings as described in the following table:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allow calls to inactive endpoints          | When selected, the call server considers inactive as well as active endpoints when attempting to resolve an address using the **Dial registered endpoints by alias** dial rule.  
Turning this option off can prevent the aliases of registrations that are no longer active from masking the aliases of endpoints registered to other call servers. This is useful in situations where an endpoint might have an active registration with one call server and an inactive registration with another (such as a mobile device that moves from a call server handling registrations through an SBC to a different call server in the network). |
| Allow calls from unregistered endpoints in territory (rogue) | When selected, the call server permits rogue endpoints to place and receive calls. Rogue endpoints are endpoints that are in sites managed by the system, but are not registered and active.  
Turning this option off blocks calls to and from rogue endpoints. This option has no effect on other unregistered network devices (such as MCUs, gatekeepers, and session border controllers) or on endpoints that are not in sites managed by the system. |
| Allow calls from unregistered endpoints out of territory | When selected, the call server permits endpoints that are not in sites managed by the system to place and receive calls.                                                                                         |
| Available bandwidth limit (percent)       | Sets the maximum percentage of the available bandwidth that can be allocated to a single call. If the requested bandwidth exceeds this value, the call server downspeeds (reduces the bit rate of) the call, but only to the user’s downspeed minimum. 
If there’s insufficient bandwidth to comply with both this setting and the downspeed minimum, the call is rejected. |
| Territory failover delay (seconds)         | The number of seconds a territory's backup cluster waits after losing contact with the primary before it takes over the territory. Must be in the range 6-300. |
| Timeout for call forwarding when no answer (seconds) | The number of seconds to wait for the called endpoint to answer (fully connect) before forwarding the call, if call forwarding on no answer is enabled for the called endpoint. Must be in the range 5-32. |
| Registration refresh interval (seconds)    | For H.323 endpoints, specifies how often registered endpoints send keep alive messages to the call server. Endpoints that fail to send keep alive messages on time are flagged as inactive. 
For SIP endpoints, specifies the refresh interval used if the endpoint didn't specify an interval or specified one greater than this value. Must be greater than or equal to the minimum SIP registration interval and in the range 150-9999. |
## Call Server Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype conference ID query timeout (seconds)</td>
<td>When integrated with a Microsoft Skype for Business environment, limits the duration of queries to the Skype for Business server for a dialed conference ID. Must be in the range 1-20.</td>
</tr>
<tr>
<td>Skype edge server discovery timeout (seconds)</td>
<td>When integrated with a Microsoft Skype for Business environment, increases or decreases the network connection timeout value when attempting to connect to the Skype for Business server to obtain MCU assignment rules. Must be in the range 1-20.</td>
</tr>
<tr>
<td>Bit rate to bandwidth conversion factor</td>
<td>The factor used to derive the bandwidth needed for a call from a specified bit rate. You can use any value from 1.000 to 5.000 (the system supports up to three decimal places of precision). This value not only affects site topology bandwidth limit calculations, but also affects bit rate and bandwidth statistics that the system reports for calls. Bandwidth calculations for H.323 calls require that the hosting MCU be actively registered to the RealPresence DMA system.</td>
</tr>
<tr>
<td>For SIP calls gatewayed to an external gatekeeper, use the H.323 email ID as the destination</td>
<td>If this option is selected, when the system uses dial rules to attempt to resolve a SIP call to an external gatekeeper, the destination in the LRQ message is set to the H.323 email ID (such as <a href="mailto:1234@example.com">1234@example.com</a>) rather than using the E.164 number alone (such as 1234). Depending on configuration and capabilities, some H.323 devices may need the full and resolvable URL of the email ID to correctly resolve the dial. If this option is off, SIP calls gatewayed to H.323 devices may fail.</td>
</tr>
</tbody>
</table>

## SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum SIP registration interval (seconds)</td>
<td>The minimum time between keep-alive messages to SIP endpoints. Must be less than or equal to the registration refresh interval and in the range 150-3600.</td>
</tr>
<tr>
<td>RFC-5626 keep-alive interval (seconds)</td>
<td>The frequency, in seconds, at which the keep-alive packet should be sent over the established static TCP/TLS channel on the firewall. This value should be lower than that of all idle connection closing timeout values on all firewalls between the RealPresence DMA system and all endpoints. Minimum value is 60 seconds. Note that the timeout value configured on the firewall must be greater than 60 seconds.</td>
</tr>
<tr>
<td>SIP CRLF keep-alive for non RFC-5626 endpoints</td>
<td>When selected, enables the RealPresence DMA system to send CRLF keep-alive pings to endpoints that do not support RFC-5626.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP CRLF keep-alive interval for non RFC-5626 endpoints (seconds)</td>
<td>If you enable <strong>SIP CRLF keep-alive for non RFC-5626 endpoints</strong>, specifies how often the RealPresence DMA system sends the keep-alive pings. Minimum value is 60 seconds. Note that the timeout value configured on the firewall must be greater than 60 seconds.</td>
</tr>
<tr>
<td>SIP options ping timer (seconds)</td>
<td>The frequency with which the system sends <strong>SIP OPTIONS</strong> requests when no other SIP traffic is received from the SIP peer. Must be in the range 1-10000. Default value is 10.</td>
</tr>
<tr>
<td>SIP options ping failure status codes</td>
<td>Specifies which responses to the <strong>OPTIONS</strong> request indicate that a SIP peer is not responsive. Valid input is a comma-separated list or dash-separated range of three-digit numeric codes; an empty field is acceptable as well. Default value is 503.</td>
</tr>
<tr>
<td>SIP max breadth</td>
<td>The maximum number of SIP peers that the system will try at once. This option applies when the Routing policy for a dial rule with the action <strong>Resolve to external SIP peer</strong> is set to <strong>All in parallel (forking)</strong>. Must be in the range 1-99. Default value is 60.</td>
</tr>
<tr>
<td>Try next SIP peer timeout (seconds)</td>
<td>The timeout in seconds when sending a <strong>SIP OPTIONS</strong> ping or an <strong>INVITE</strong> to a SIP peer. This value can be a numeric value in the range 0.1-31.0. Default value is 5.0.</td>
</tr>
<tr>
<td>SIP peer dial rule timeout (seconds)</td>
<td>The number of seconds after invoking the dial rule that the dial attempt is canceled. Must be in the range 1-300. Default value is 25.</td>
</tr>
<tr>
<td>Nonresponsive SIP peer status codes</td>
<td>Specifies which responses to an initial <strong>SIP INVITE</strong> indicate that a SIP peer is not responsive. Valid input is a comma-separated list or dash-separated range of three-digit numeric codes; an empty field is acceptable as well. Default value is 503.</td>
</tr>
<tr>
<td>Allow offer-less INVITE to endpoint (upstream)</td>
<td>If this option is selected, when the RealPresence DMA system originates a SIP call and performs a dial-out, the system can send an offer-less <strong>INVITE</strong> to the dialed endpoints. <strong>Offer-less INVITES</strong> (per RFC 3261 and RFC 3264) notify the endpoint of the upcoming call, but don’t exchange media information first. The endpoint must provide initial media information back in its responses. The far end of the call is then contacted with the endpoint's &quot;offer&quot; and the media is finalized. Some endpoints don’t correctly support offer-less INVITES. If calling compatibility issues occur, this option should be turned off.</td>
</tr>
</tbody>
</table>
### H.323 Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Gatekeeper call mode                                     | **Direct call mode** - The call server processes only H.225.0 RAS call control messages. The endpoints exchange other call signaling and media control messages directly, bypassing the gatekeeper.  
**Routed call mode** - The call server proxies all H.323 signaling messages. Default setting on newly-installed core systems. |
| Accept H.323 neighbor requests only from specified external gatekeepers | If this option is selected, the call server accepts H.323 location requests (LRQs) only from gatekeepers configured on the External Gatekeeper page. |
| Resolve H.323 Email-ID dial strings to other registered H.323 aliases | If this option is selected, the call server resolves email ID dial strings to another local alias by using the user part of the email address.  
For example, the dial string [1234@mycompany.com](mailto:1234@mycompany.com) would resolve to the endpoint registered as 1234. |
| Automatically assign enterprise users’ email addresses as H.323 email IDs | If this option is selected and the system is integrated with Active Directory, an endpoint associated with an enterprise user is assigned the user’s email address (if that address hasn’t already been explicitly assigned to another endpoint). |
| Location request hop count                               | The initial hop count the call server uses when it sends LRQs to neighbored gatekeepers.                                                       |
| Location request timeout (seconds)                       | The number of seconds to wait for a response from a neighbored gatekeeper.                                                                     |
| IRQ sending interval (seconds)                           | The interval at which the system sends IRQ (Information Request) messages to H.323 endpoints in a call, requesting QoS (Quality of Service) reports.  
Must be in the range 10-600. |
| Terminate calls based on failed responses to IRQs        | If selected, the call server terminates a call if it sends an IRQ to an endpoint that signaled support for IRQs, and the endpoint either fails to respond or responds with an IRR (Information Request Response) containing an `invalidCall` field. This prevents a call license from being used unnecessarily for a call that's no longer active.  
Some endpoints signal support for IRQs but don't correctly handle IRQ/IRR messaging, causing active calls to be disconnected if this option is selected. If this problem occurs with endpoints, it's recommended to leave this option off.  
This setting has no effect on calls from endpoints that don't signal support for IRQs. |
Dynamically blacklist signaling from hyperactive endpoints

If selected, the call server adds H.323 endpoints to its blacklist (ignoring their signaling messages) when they send duplicate RRQ or GRQ messages in excess of the criteria you specify below.

When an endpoint is blacklisted, the call server:
- Stops interpreting, responding to, auditing, or logging messages of that type from the endpoint
- Creates Alert 5003 and corresponding SNMP trap
- Logs the blacklisting

Gatekeeper Blacklist Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message type</td>
<td>You can specify the blacklist settings separately for RRQ (Registration Request) and GRQ (Gatekeeper Request) messages.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of duplicate messages within the specified interval that causes an endpoint to be blacklisted.</td>
</tr>
<tr>
<td>Interval (msec)</td>
<td>The interval in milliseconds to which the threshold applies.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>If this option is selected, endpoints that are blacklisted are also quarantined. They remain in Quarantined or Quarantined (Inactive) status (unable to make or receive calls) until manually removed from quarantine.</td>
</tr>
<tr>
<td>Apply to VBP</td>
<td>If this option is selected, video border proxies (VBPs) can be blacklisted. If a VBP is blacklisted, none of the endpoints behind it can register.</td>
</tr>
</tbody>
</table>
| Remove non-hyperactive endpoints from blacklist after specified interval (minutes) | The interval after which an endpoint is removed from the blacklist and is once again allowed to register. When an endpoint is removed from the blacklist, the call server:
  - Starts interpreting, responding to, auditing, and logging messages of that type from the endpoint
  - Clears the alert and SNMP trap
  - Logs the removal from the blacklist
  If the endpoint was quarantined as well as blacklisted, it remains quarantined. |
| Registration sharing settings              | See Registration Sharing.                                                   |

3. Click **Update** to save the settings.

**Related Links**
- Registration Sharing on page 303
- Names and Aliases in a Mixed H.323 and SIP Environment on page 530
Registration Sharing

The RealPresence DMA system supports sharing of endpoint registrations from an edge-configured system to another edge-configured system (for example, in a VPN tunnel configuration) or a core-configured system.

A RealPresence DMA edge system functions as a gatekeeper and all public endpoints will register via SIP or H.323 with the edge system. To enable calls from an edge system to another edge system or to a core system, and vice versa, you must configure registration sharing on the edge system(s). When you do so, registrations received by the edge system are shared with the core system via the core system's REST API. Note that you must also configure external H.323 neighbored gatekeepers and external SIP peers to enable calls from the edge system to the core system.

With registration sharing enabled, an edge system will share the following information with another edge system or a core system:

▪ New and refreshed registrations
▪ Terminated registrations
▪ Blocked registrations
▪ Deleted registrations
▪ Quarantined registrations

After registration sharing occurs, the **Endpoints** page on the RealPresence DMA core system displays the IP address of the edge system for shared endpoint registrations instead of the IP address of the individual endpoints.

Shared registration information is available across a supercluster. Registration sharing from a RealPresence DMA core system to an edge system is not supported.

---

**Note:** If the RealPresence DMA core system loses its connection with the edge system that's sharing registrations, the core system must be the primary cluster owner of a Territory for shared registrations to time out appropriately on that core system.

---

**Related Links**

[Configure the Call Server](#) on page 297

---

**Configure Registration Sharing**

When you initially enable registration sharing on the RealPresence DMA edge system, it performs a bulk sharing of registrations with the other edge system or core system.

After the bulk sharing, individual registrations on the edge system are shared incrementally with the other edge system or core system. If you disable registration sharing, the next time you enable it, the edge system will again perform a bulk sharing of registrations with the other edge system or core system.

After you configure registration sharing, if a caller can't dial out to a SIP registered endpoint, make sure that the endpoint doesn't use the same address of record (AOR) to register to both the edge system and the core system. If this happens, you must change the user name used in the registration of the SIP endpoint on either the core system or edge system. You should then delete the endpoints from both the core system and edge system and allow the endpoints to display after they register with unique names.

With registration sharing enabled on the edge system, deleted registrations are typically reflected right away on the other edge system or core system. However, if you disable registration sharing, some registrations may persist on the other system. You can configure the number of days after which the other system will delete inactive registrations. The default setting is 30 days but you can specify a different number in the **Registration Sharing Settings**.
Procedure

1. On a RealPresence DMA edge-configured system, go to Service Config > Call Server Settings.
2. In Registration Sharing Settings, select Share registrations with another DMA.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration sharing destination hostname</td>
<td>The FQDN of another RealPresence DMA edge-configured system or a core-configured system.</td>
</tr>
<tr>
<td>Registration sharing port number</td>
<td>The REST API port number of the RealPresence DMA edge-configured or core-configured system.</td>
</tr>
<tr>
<td>Registration sharing user name</td>
<td>The user name used to log into the REST API on the RealPresence DMA edge-configured or core-configured system. The user must have Administrator or Provisioner permissions.</td>
</tr>
<tr>
<td>Registration sharing password</td>
<td>The password used to log into the REST API on the RealPresence DMA edge-configured or core-configured system. The user must have Administrator or Provisioner permissions.</td>
</tr>
<tr>
<td>Number of days until inactive shared registrations are deleted</td>
<td>When selected, the number of days after which the RealPresence DMA edge-configured or core-configured system will delete inactive registrations.</td>
</tr>
</tbody>
</table>

4. Select Update to save the settings.
Dial Plans

Topics:

- Dial Rules
- Default Dial Plan
- Add a Dial Plan
- Add a Dial Rule to a Dial Plan
- Override SIP Transport Protocol in Dial Rules
- Edit a Dial Rule
- License Sharing and Direct Call Routing
- Auto Dial-out Cascading to Cloud Service-based Conferences
- Associating a Dial Plan to a Call Service
- Test a Dial Plan

Dial plans control how the RealPresence DMA system's call server uses dial strings to determine where to route calls.

You can associate different dial plans for individual call services such as H.323, SIP, or WebRTC. You can also associate specific dial plans to calls received from guest ports.

This flexibility allows you to assign different dial plans to separate SIP servers, neighbored gatekeepers, or session border controllers within your video conferencing environment.

The system comes with two dial plans out-of-the-box: a default dial plan and a guest dial plan. The Default Dial Plan provides the most commonly needed address resolution processing and is used for authorized calls. The Guest Dial Plan is used for unauthorized guest calls and contains no dial rules. The Guest Dial Plan blocks all guest calls unless you add dial rules to it to allow unauthorized calls.

You can add additional dial plans as needed. You can also add, edit, remove, and change the order of the dial rules that are included in the default dial plan. Dial strings may match multiple dial rules, but the rules have a priority order. When the RealPresence DMA system receives a call request and associated dial string, it applies the first matched (highest priority) dial rule within the associated dial plan.

You can test a dial plan using the Test Dial Plan action. You can specify various caller parameters and a dial string, and see how the selected dial rules handle such a call.

Related Links
Default Dial Plan on page 306

Dial Rules

Dial rules specify how the RealPresence DMA system call server uses a dial string to determine where to route a call.

The dial string may include an IP address, a string of numbers that begin with a prefix associated with a service, a string that begins with a country code and city code, or a string that matches a particular alias for a device.
Dial strings may match multiple dial rules, but the rules have a priority order. When the RealPresence DMA system call server receives a call request and associated dial string, it applies the first matched (highest priority) dial rule.

A dial rule consists of an optional preliminary script to modify dial strings and the action to be performed, which you select from a defined list of actions. The actions apply dial resolution logic.

For example, the Resolve to registered endpoint action applies all the associated system configurations and performs various searches on the internal endpoint registration records to determine if the inbound call is attempting to reach another registered endpoint. It automatically adjusts for signaling protocol, case, and standard dial string deviations to locate a registered endpoint. You don’t have to account for these variables in your dial plan because the logic behind the dial rule action does so for you.

Default Dial Plan

The RealPresence DMA system is configured by default with a generic dial plan that covers many common call scenarios.

The following table describes the default dial plan:

<table>
<thead>
<tr>
<th>Default Rule Description</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Dial registered endpoints by alias</td>
<td>If the dial string is the alias or SIP URI of a registered endpoint, the call is routed to that endpoint.</td>
</tr>
<tr>
<td>2 Dial by conference room</td>
<td>If the dial string is the dial-in number of a conference room on the RealPresence DMA system, the call is routed to that conference room.</td>
</tr>
<tr>
<td>3 Dial to SIP conference factory</td>
<td>If the dial string is the dial-in number of a SIP conference factory, the call is routed to that SIP conference factory.</td>
</tr>
<tr>
<td>4 Dial by virtual entry queue ID</td>
<td>If the dial string is the dial-in number of a virtual entry queue on the RealPresence DMA system, the call is routed to that VEQ.</td>
</tr>
<tr>
<td>5 Dial to on-premises RealConnect™ conference</td>
<td>If the dial string is the dial-in number of a Skype for Business conference on the Skype AVMCU, the call is routed to an available Polycom MCU that supports Skype for Business and is automatically connected to the corresponding Skype conference on the AVMCU. If no Polycom MCUs that support Skype for Business are available, the conference fails to start. This rule is disabled by default.</td>
</tr>
<tr>
<td>6 Dial services by prefix</td>
<td>If the dial string begins with the configured prefix of a service (such as an MCU, ISDN gateway, SBC, neighbor gatekeeper, SIP peer proxy, or simplified ISDN dialing service) the call is routed to that service.</td>
</tr>
</tbody>
</table>

**Note:** For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to alice@polycom.com must be one of the following:

- sip:123alice@polycom.com
- 123alice
<table>
<thead>
<tr>
<th>Default Rule Description</th>
<th>Effect</th>
</tr>
</thead>
</table>
| 7 Dial external networks by H.323 URL, Email ID, or SIP URI   | If the address is an external address, the call is routed to that external address (H.323 and SIP calls use the designated SBC for the originating site to reach addresses outside the enterprise network). Examples of external addresses:  
  johnsmith@someothercompany.com  
  sip:johnsmith@someothercompany.com                                                                 |
| 8 Dial endpoints by IP address                                | If the address is an IP address, the call is routed to that IP address (H.323 calls use the designated SBC for the originating site to reach addresses outside the enterprise network). Examples of IP addresses:  
  1.2.3.4 1.2.3.4##abc sip:abc@1.2.3.4 sip:1.2.3.4@mycompany.com                                                                 |
| 9 Dial to RealConnect conference by external Skype system conference ID | If the dial string is the dial-in number of a Lync or Skype conference on an external Lync or Skype system, the call is routed to an available Polycom MCU that supports RealConnect conferences for external Lync or Skype systems. If no Polycom MCUs that support RealConnect conferences for external Lync or Skype systems are available, the conference fails to start.  
  Note: This rule is disabled by default, but is required if any external Lync or Skype systems are defined. |

**Related Links**
- [Dial Plans](#) on page 305
- [Suggestions for Modifying the Default Dial Plan](#) on page 307

**Suggestions for Modifying the Default Dial Plan**

If you have special configuration needs and want to modify the default dial plan, be aware that some of the default dial rules are necessary for normal operation.

Removing or modifying them takes the system out of compliance with ITU and IEEE standards.

Consider the following suggestions and guidelines if you modify the dial plan:

- Polycom recommends ordering dial rules so that the rule with the action **Resolve to external SIP peer** appears last in the list. If a dial rule with the action **Resolve to external SIP peer** doesn't successfully route a call, the call is aborted and no subsequent dial rules will be attempted. Polycom also recommends that this rule not appear higher than its default order in the list of dial rules, because this can prevent valid aliases, VMRs, and VEQs from being dialed and can result in reduced system performance.
  - To add an MCU, ISDN gateway, SBC, neighbor gatekeeper, SIP peer, or simplified dialing service that can be dialed by prefix, configure the prefix range of the new service on the appropriate page. No dial plan change is necessary, since the rule **Dial services by prefix** of the default dial plan takes care of dialing by prefix.
- You can remove or disable a default dial rule if you don't want the associated functionality.
Note that the rule **Dial endpoints by IP address** is used in several scenarios where calls are received from neighbor gatekeepers or SBCs. Removing it breaks these scenarios.

- If certain dial strings are matching on the wrong dial rule, you may need to re-order the rules.
- In some circumstances (depending on the dial plan and the network topology and configuration), dial rules using the **Resolve to external address** action or the **Resolve to IP address** action can enable dialing loops to develop, especially if servers reference each other either directly or via DNS. Common ways to avoid dialing loops include:
  - Use domain restrictions to ensure that the RealPresence DMA system and its peers are each responsible for specific domains.
  - Use a preliminary script like the sample script **SUBSTITUTE DOMAIN (SIP)** to change the domain of a SIP URI dial string to something that will not create a dialing loop.
  - Use a preliminary script to change the domain before sending to a peer.
  - Use configuration options on the peers to prevent loops.
  - Create a dial rule that uses the **Block** action and a preliminary script to enhance the system's ability to prevent dialing loops for specific types of calls. The preliminary script ensures that the dial rule only matches the types of calls you want to block. This dial rule should be ordered after other dial rules that are expected to resolve the intended call requests.

  For example, a dial rule with the **Block** action using the following preliminary script blocks all call requests that use a prefix of 44 if they have not been resolved by previous dial rules:

  ```java
  println("DIAL STRING=" + DIAL_STRING);
  var prefix='44'
  var re = RegExp('^(sip:|sips:|h323:|tel:)?' + prefix +'.*')
  if(! DIAL_STRING.match(re))
  {
    println("NEXT RULE");
    return NEXT_RULE;
  }
  println("ACCEPT and terminate 44 prefix calls if they were not resolved by previous dial rules");
  ```

- You can add a filtering preliminary script to any dial rule to restrict the behavior of that rule.

  For example, if you know that all the aliases of a specific neighbor gatekeeper are exactly 10 digits long, you may want to route calls to that gatekeeper only if the dial string begins with a certain prefix followed by exactly 10 digits.

  To accomplish this, add a preliminary script to the service prefix dial rule that rejects all dial strings that begin with the prefix, but aren't followed by exactly 10 digits.

- To exclude certain dial strings, combine a filtering preliminary script with the **Block** action.

- You can use a preliminary script to modify the dial strings accepted by any of the rules.

  For example, to be able to call an enterprise partner by dialing the prefix 7 followed by an alias in the partner's namespace, configure a **Resolve to external** that transforms the string 7xxxx to xxxx@enterprisepartner.com.

  This type of dial string modification is also useful if you're using Skype for Business conference dial strings with prefixes. To route a dial string with a prefix to a Skype conference ID, configure a **Resolve to Skype conference ID** action with a preliminary script that removes the prefix from the dial string (1234567 would become 4567, for example).

- If your enterprise includes another gatekeeper and you want to route calls to that gatekeeper without a prefix, add a dial rule using the **Resolve to external gatekeeper** action.
▪ If your enterprise includes a SIP peer and you want to route calls to that peer without a prefix, add a
dial rule using the **Resolve to external SIP peer** action.

If you have multiple SIP peers, a call matching the rule is routed to the first one to answer. You may
want to specify the domain(s) for which each is responsible.

When routing to a SIP peer, the RealPresence DMA system gives up its ability to route the call to
other locations if the peer rejects the call. Consequently, a dial rule using the **Resolve to external
SIP peer** action should generally be the last rule in the dial plan.

▪ In a mixed H.323 and SIP environment, the RealPresence DMA system acts as a seamless
gateway. If an H.323 device sends it a location request (LRQ) and the dial plan contains a dial rule
using the **Resolve to external SIP peer** action, the RealPresence DMA system will respond with a
location confirm (LCF) because it can resolve the address by routing the H.323 call through its
gateway to the SIP peer(s). You can prevent H.323 calls from being routed to SIP peers by
restricting which calls are routed to them in one or more of the following ways:
  ◦ Assign each SIP peer an authorized domain or domains (This helps avoid dialing loops).
  ◦ Assign each SIP peer a prefix or prefix range.
  ◦ Add a preliminary script to the dial rule using the **Resolve to external SIP peer** action that
    ensures that the rule will only match a SIP address.
  ◦ Make the dial rule using the **Resolve to external SIP peer** action the last rule and ensure
    that all H.323 calls will match against one of the preceding dial rules.

**Related Links**

- **Default Dial Plan** on page 306
- **Alert 5004** on page 593

**Add a Dial Plan**

You can create a new dial plan to be associated with one or more call services such as H.323, SIP, or
WebRTC.

After you create the dial plan, you need to add dial rules and prioritize them.

**Procedure**

1. Go to **Service Config > Dial Plan > Dial Plans** and click **Add Dial Plan**.
2. Enter a **Dial plan name** and click **OK**.

**Add a Dial Rule to a Dial Plan**

You can add a dial rule to a dial plan and prioritize the dial rule.

When the RealPresence DMA system receives a call request and associated dial string, it applies the first
matched (highest priority) dial rule within the associated dial plan.

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. Select the dial plan to which you want to add a rule and select **Add Dial Rule**.
3. Enter a detailed **Description** of the rule.
4. Select the **Action** the rule will perform.

The following table describes the **Action** options and how the system attempts to resolve the destination
address (dial string) for each action:
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Blocks the call.</td>
</tr>
<tr>
<td>Resolve to IP address</td>
<td>Attempts to treat the dial string as an IP address, and if it can, assumes it's the address (and port, if included) of an unregistered endpoint. If no port is specified, it uses the default port of the signaling protocol. If the dial string contains the characters ##, it tries to do this using the characters before ##. For SIP: • If the host part is an IP address:   ◦ If it belongs to one of the systems in the supercluster, the system examines the user part.   ◦ If it belongs to a local domain, the dial string is resolved unchanged.   ◦ If it belongs to neither of the above, the dial string is resolved unchanged. • If the host part is a hostname or domain:   ◦ If it belongs to one of the systems in the supercluster, the system examines the user part.   ◦ If it belongs to a local domain, the system examines the user part.   ◦ If it belongs to neither of the above, the dial string is passed to the next dial rule. • When the system examines the user part, it takes one of the following actions:   ◦ If the user part is an IP address, it resolves the call to that IP address. For example, the dial string sip:1.2.3.4@10.1.1.1 would be resolved to sip:1.2.3.4.   ◦ If the user part contains ## and the preceding characters are an IP address, the characters after ## are treated as the user part of a URI. For example, if the user part has the format ip-addr##string, the system resolves the call to the dial string sip:string@ip-addr. • The user part examination fails (and the dial string is passed to the next dial rule) if the user part isn't in one of the following formats:   ◦ IP address   ◦ IP address##   ◦ IP address##string For H.323, if the characters before the first ## resolve to an IP address, the characters after that are converted into the destinationInfo (ACF) or destinationAddress (Setup) as follows: • If possible, encoded as a dialedDigits address. • Otherwise, if possible, encoded as a url-ID. • Otherwise, encoded as an h323-ID.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resolve to service prefix</td>
<td>Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name. For instance, if the SIP peer's prefix is 123, the dial string for a call to <a href="mailto:alice@polycom.com">alice@polycom.com</a> must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• sip:<a href="mailto:123alice@polycom.com">123alice@polycom.com</a></td>
</tr>
<tr>
<td></td>
<td>• 123alice</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resolve to conference ID by Skype query</td>
<td>Queries an integrated Skype SIP peer for a Skype AVMCU-based conference with a matching conference ID. This dial rule action enables Polycom RealConnect functionality for Skype on-premise systems only; it does not apply to external Skype systems. When selected, the following fields are available:</td>
</tr>
<tr>
<td></td>
<td>• Conference template</td>
</tr>
<tr>
<td></td>
<td>When checked, you can select the conference template used to start the conference. If you leave this option unchanged, the Default conference template configured in Admin &gt; Conference Manager &gt; Conference Settings will be used. Keep in mind that the conference template must specify a Conference mode of AVC only, or the conference won’t start.</td>
</tr>
<tr>
<td></td>
<td>• MCU pool order</td>
</tr>
<tr>
<td></td>
<td>When checked, select the MCU pool order to use for MCUs that provide Skype AVMCU cascade functionality. When the dial rule initiates a new RealPresence DMA conference, one of the selected external SIP peers resolves the conference ID. The RealPresence DMA system then uses the MCU pool order configured for the external SIP peer that hosts the conference to select an MCU. If no MCU pool order is configured for the external SIP peer that hosts the conference, the dial rule uses the MCU pool order you select in this field to route the conference to an MCU. If you leave this option unchecked, the dial rule will use the default pool order selected in the Default MCU pool order field on the Admin &gt; Conference Manager &gt; Conference Settings page.</td>
</tr>
<tr>
<td></td>
<td>• MCU Affinity</td>
</tr>
<tr>
<td></td>
<td>When checked, you can select the MCU Affinity as follows:</td>
</tr>
<tr>
<td></td>
<td>▪ Prefer MCU in first MCU pool</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on. This setting is recommended to help ensure that the MCU selected is optimal based on its geographic proximity to the Skype AVMCU.</td>
</tr>
<tr>
<td></td>
<td>▪ Prefer MCU in first caller’s site</td>
</tr>
<tr>
<td></td>
<td>Matches the MCU chosen for the call with the site that the first caller’s endpoint belongs to.</td>
</tr>
<tr>
<td></td>
<td>When not checked, defaults to the value in the MCU Selection field on the Admin &gt; Conference Manager &gt; Conference Settings page.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Available SIP peers > Selected SIP peers selection area** | This area lists the names of Available SIP peers and any Selected SIP peers. With the provided arrow buttons, you can move SIP peers between the areas. When the dial rule is executed, the system will query the selected SIP peers to find which one is hosting the Skype conference. **Note:** For an external SIP Peer to be listed in the Available SIP peers area, it must be listed on the Network > External SIP Peers page and have the following configuration:  
  - A Type of Microsoft  
  - The Enable RealConnect conferences check box selected in the Skype Integration tab |
| **Resolve to Skype Conference ID by Conference Auto Attendant** | Examines the beginning of the dial string, searching for the longest matching prefix of a defined external Skype system. If a match is found, the dial rule removes the prefix from the dial string and passes the resulting conference ID to the Polycom MCU, which then contacts the CAA of the matched external Skype system.  
If an external Skype system is listed on the Integrations > External Skype Systems page, it's available in the Available external Skype systems box. You can move external Skype systems to which the rule applies to the Selected external Skype systems box.  
A dial rule with this action is required for Polycom MCUs to connect to Skype conferences on external Skype systems. |
| **Resolve to external SIP peer** | Checks the domain of the dial string against all of the rule's selected peers, looking for a peer proxy responsible for that domain. If the dial string matches the domain of one of the selected SIP peers, this rule will either successfully route the call, or the call will be aborted; no subsequent dial rules are attempted.  
After selecting this action for a rule, select a Routing policy. The policy affects the way the system resolves dial strings to SIP peers:  
  - **All in parallel (forking)**  
    The system uses all SIP peers simultaneously to try to resolve the dial string.  
  - **Weighted round-robin**  
    You can assign each SIP peer a weight in the range 1-100, with a higher weight giving a SIP peer higher priority; the system tries each SIP peer sequentially according to the SIP peer's assigned weight. You can assign a SIP peer different weights in different dial rules.  
    After choosing a routing policy, move the SIP peers to which the rule applies from the Available SIP peers box to the Selected SIP peers box. If the Weighted round-robin routing policy is selected, choose a weight for the selected SIP peer using the Edit weight button.  
**Note:** This action employs the H.323<>SIP gateway function if applicable. |
### Action | Description
--- | ---
Resolve to external gatekeeper | If the dial string appears to be an H.323 alias, simultaneously sends LRQ messages to all of the rule’s selected gatekeepers. After selecting this action for a rule, move the gatekeepers to which the rule applies from the **Available gatekeepers** box to the **Selected gatekeepers** box. **Note**: This action employs the H.323<->SIP gateway function if applicable.

Resolve to external address | Determines if the dial string is a well-formed instance of an external address type to which the rule applies, and if so, uses the resolution procedures specified in the applicable standard for that address type. After selecting this action for a rule, select the address type or types to which the rule applies. The address types and applicable standards used to resolve them are:
- **SIP URI** - RFCs 3261 and 3263
- **H.323 url-ID** - H.323 specification, Annex O
- **H.323 Email-ID** - H.225.0 specification, Appendix IV

Resolve to registered endpoint | Looks for a registered endpoint (active or inactive) that has the same alias or signaling address. **Note**: This action employs the H.323<->SIP gateway function if applicable.

Resolve to conference room | Looks for a conference room (VMR) that matches the dial string.

Resolve to SIP conference factory | Determines if the dial string contains a SIP conference factory ID and, if so, creates a multi-point conference on an MCU and generates a conference ID for the conference. The conference IDs are strings that can be dialed by any endpoint (SIP or H.323) to join the conference.

Resolve to virtual entry queue | Looks for a shared-number entry queue that matches the dial string.

### Procedure
1. In the **Preliminary** tab, add a preliminary script. A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule’s action is performed.
2. Select the **Enabled** check box.
3. Type (or paste) the preliminary script you want to apply.
4. Click **Debug this Script** to open the **Script Debugging** window.
5. Specify the parameters of a call and the dial string, and assess what effect the script has on the dial string:
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dial string            | The `DIAL_STRING` variable in the script, which is initially set to the dial string being evaluated. Enter a dial string to test. Alternatively, provide the entire `SIP INVITE` message. Then click **Execute Script**.  
**Note:** For SIP, the script should always specify the schema prefix (sip or sips). For instance: `DIAL_STRING = "sip:xxx@10.33.120.58"` |
| Caller site            | Select a site to set the first four caller variables.                                                                                                                                                  |
| Caller variables       | Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable.                                                                   |
| VMR/transient conf ID  | Specifies the return value of the function `getConferenceRoomOrID()` .  
If the script simulates a call to a VMR or transient conference ID or a dial-in call, this field is blank.                                                                                       |
| Final result           | Displays the outcome of running the script.  
For a dial rule preliminary, if the script rejected the dial string (skipping the dial rule action and passing it on to the next dial rule), a message tells you so. Otherwise, the transformed dial string is displayed. |
| Script output          | Displays any output produced by the script (for example, `println` statements).                                                                                                                      |
| Output SIP headers     | For an external SIP peer’s postliminary, displays the headers produced by the script.                                                                                                                 |

6. **Click** **Execute Script** **to test your preliminary script.**

**Related Links**

- [*External H.323 Gatekeepers*](#) on page 156
- [*Sample Preliminary and Postliminary Scripts*](#) on page 349

## Override SIP Transport Protocol in Dial Rules

In certain dial rules, you can select a SIP transport protocol that the RealPresence DMA system uses for outbound dialing that’s different from the originating endpoint’s protocol.

Using the override option for the SIP transport protocol on edge and combination systems that dial out to external addresses helps prevent call denials to originating endpoints. The systems attempt to use other protocols to connect calls to external destinations.

You can override the SIP transport protocol of an originating endpoint in dial rules that have the following actions:

- Resolve to IP address
- Resolve to external address
Note: When you select an override protocol, the RealPresence DMA system uses that protocol (or multiple protocols in a specific order) to attempt to connect a call to the destination. If the connection fails, then the call fails.

Procedure

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. Select the dial plan that needs the new rule.
3. In the **Dial Rules** section, select **Add Dial Rule**.
   You can also edit an existing dial rule.
4. Configure the following settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description of the rule.</td>
</tr>
<tr>
<td>Action</td>
<td>Select <strong>Resolve to IP address</strong> or <strong>Resolve to external address</strong>.</td>
</tr>
<tr>
<td>Relay Media</td>
<td>Select this options if you want the edge or combination system to relay</td>
</tr>
<tr>
<td></td>
<td>media to the call destination.</td>
</tr>
<tr>
<td>Use SIP URI</td>
<td>If you select <strong>Resolve to external address</strong> as the rule action, choose the</td>
</tr>
<tr>
<td>Use H.323 url-ID</td>
<td>external address types to which the rule applies.</td>
</tr>
<tr>
<td>Use H.323 email-ID</td>
<td></td>
</tr>
<tr>
<td>SIP Transport</td>
<td>Select <strong>SIP Transport</strong>, then choose the transport protocol the RealPresence</td>
</tr>
<tr>
<td></td>
<td>DMA system will use to override the protocol from the origination endpoint:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with UDP</strong>: The system connects the call to the destination</td>
</tr>
<tr>
<td></td>
<td>over UDP. If the connection fails, the call fails.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with TCP</strong>: The system connects the call to the destination</td>
</tr>
<tr>
<td></td>
<td>over TCP. If the connection fails, the call fails.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Override with TLS</strong>: The system connects the call to the destination</td>
</tr>
<tr>
<td></td>
<td>over TLS. If the connection fails, the call fails.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Auto Detect</strong>: The system uses DNS to select the protocol (as specified</td>
</tr>
<tr>
<td></td>
<td>in RFC 3263). If the next hop is a numeric IP address instead of a host</td>
</tr>
<tr>
<td></td>
<td>or domain name, the system uses the transport protocols in the following</td>
</tr>
<tr>
<td></td>
<td>order to connect to the call destination: originating endpoint’s protocol,</td>
</tr>
<tr>
<td></td>
<td>TLS, TCP, UDP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Try All</strong>: The system overrides the SIP transport protocol from the</td>
</tr>
<tr>
<td></td>
<td>originating endpoint and instead uses the transport protocols in the</td>
</tr>
<tr>
<td></td>
<td>following order to connect to the call destination: TLS, TCP, UDP.</td>
</tr>
</tbody>
</table>

5. Select **OK**.
Edit a Dial Rule

You can edit a dial rule within a dial plan.

You can update the preliminary script or the action used, or you can disable the rule.

Procedure

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan to which the dial rule belongs.
3. Select the rule you want to edit and click Edit Dial Rule.
4. Revise the fields as described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial Rule</td>
<td>Clearing this check box lets you turn off a rule without deleting it.</td>
</tr>
<tr>
<td>Enabled</td>
<td>The text description displayed on the Dial Rules page.</td>
</tr>
<tr>
<td>Description</td>
<td>The action to be performed. When you select some actions, additional settings become available.</td>
</tr>
<tr>
<td>Action</td>
<td>A preliminary is an executable script, written in the JavaScript language, that defines processing actions (filtering or transformation) that are part of a dial rule and may be applied to a dial string before the dial rule's action is performed.</td>
</tr>
<tr>
<td>Preliminary</td>
<td>Lets you turn a preliminary on or off without deleting it.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Type (or paste) the preliminary script you want to apply. Then click Debug this Script to test the script with different variables.</td>
</tr>
</tbody>
</table>

5. When finished, click OK.

License Sharing and Direct Call Routing

A license-sharing API enables a RealPresence DMA edge system to borrow a license from a core system.

When an outside endpoint registered to an edge system calls another outside endpoint registered to an edge system or a Video-as-a-Service (VaaS) conference (for example, Microsoft Teams), the edge system checks for an available call license. If the edge system doesn’t have one, it borrows a license from the core system and directly routes the call to an outside endpoint address or VaaS conference.

To enable the RealPresence DMA edge system to correctly route calls to a VaaS conference, you need to enable registration sharing and configure two dial rules on the edge system.
Add Dial Rules to Directly Route Calls to a VaaS Conference

You can configure two dial rules on a RealPresence DMA edge system to enable direct routing of calls to a Video-as-a-Service (VaaS) conference.

For license sharing between a RealPresence DMA edge system and core system to work, you need to configure registration sharing on the edge system.

To enable the RealPresence DMA system to correctly route VaaS calls, you need to configure one dial rule for the H.323 public dial plan and one for the SIP public dial plan. If an incoming call to the edge system matches one of these dial rules, the edge system directly routes the call to the VaaS conference.

Procedure

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. Select **H.323 Dial Plan Public**.
3. Under **Dial Rules**, select the **Add** button.
4. Enter a brief **Description** of the dial rule.
5. In the **Action** field, select **Resolve to external address**.
6. Select the following options:
   a. **Relay Media**
   b. **Use SIP URI**
   c. **Use H.323 URL-ID**
   d. **Use H.323 email ID**
7. Select the **Preliminary** tab.
8. Enter a script to enable correct routing for VaaS calls. You must revise the following sample script as needed for your environment:

   ```javascript
   if (!(DIAL_STRING.match("<your-companies-Microsoft-Teams-Domain>")||DIAL_STRING.match("webex.com") || DIAL_STRING.match("zoomcrc.com"))
   { println("not Teams or Webex or Zoom call"); return NEXT_RULE; }
   ```

9. Click **OK** to add the new dial rule.
10. Select **SIP Dial Plan Public**.
11. Repeat steps 3-9.

Auto Dial-out Cascading to Cloud Service-based Conferences

The RealPresence DMA system supports cloud video interoperability by providing auto dial-out cascading to conferences hosted by cloud-based Video as a Service (VaaS) providers such as Microsoft Teams.

The auto dial-out cascade feature can be configured on RealPresence DMA core-configured or combination-configured systems by creating a dial rule that, when matched, creates an auto dial-out cascade link to a cloud service-based video conference.

When a call into the RealPresence DMA system matches the dial string configured in the cascade dial rule, the system creates a conference on a local RealPresence Collaboration server, which then creates an auto dial-out cascade to a conference hosted by a VaaS provider. For Microsoft Teams conferences,
the dial-out cascade connects to a Teams conference through the Polycom RealConnect for Clariti for Microsoft Teams service.

The auto dial-out cascade feature can save network bandwidth. When multiple participants dial directly into a cloud service-based conference, each call consumes additional bandwidth. An auto dial-out cascade link from an MCU to the conference requires only one link per conference for numerous participants.

The following information applies to auto dial-out cascade conferences:

- If the dial-out cascade link between the MCU and the cloud service-based conference disconnects, the cascade link will not be re-established. Participants on the MCU have no indication when a cascade link is disconnected; all participants must drop the call and rejoin the conference to re-establish the cascade link to the cloud video service.

- Participants in a dial-out cascade conference may hear MCU audio announcements such as the Welcome message. To resolve this issue, see Prevent an MCU from Playing Audio Announcements During an Auto Dial-out Cascade Conference.

- For dial-out cascade calls to cloud-based VaaS conferences, including Microsoft Teams conferences, IVR service is not supported on the VaaS service or on the MCU.

### Register MCUs for Auto Dial-out Cascading

For auto dial-out cascading into cloud-based video conferences to work, you need to register MCUs with the RealPresence DMA system.

If you select a specific pool order when you add the auto dial-out cascade dial rule, you need to register each MCU in the pools within the pool order as an H.323 gatekeeper in the RealPresence DMA system. Registering each MCU as a SIP proxy is optional. You must register MCUs from Polycom RMX Manager.

**Procedure**

1. Go to the RMX Manager system web interface.
2. Register each MCU that will be used for cascading into a cloud service-based video conference as an H.323 gatekeeper or SIP registrar in the RealPresence DMA system.
   - Use the private signaling IP address of the RealPresence DMA edge or combination system as the H.323 gatekeeper or SIP registrar IP address.

### Add a Dial Rule for Auto Dial-Out Cascading to a Cloud Service-Based Conference

An auto dial-out cascade dial rule enables registered endpoints to call into cloud service-based video conferences. You can add the cascade dial rule in RealPresence DMA core-configured or combination-configured systems.

When a call into the RealPresence DMA system matches the dial string configured in the cascade dial rule, the system creates a conference on a local MCU. The MCU then creates an auto dial-out cascade to a conference hosted by a VaaS provider. For Microsoft Teams conferences, the cascade connects to a Teams conference through the Polycom RealConnect for RealPresence Clariti solution for Microsoft Teams service.

You can add multiple cascade dial-out dial rules. For example, to host multiple customers, you can create dial rules that each include a customer’s domain or specific tenant ID.

To enable calls from unregistered endpoints, see Calls from Unregistered Endpoints to Cloud Service-based Conferences.
Note: In the auto dial-out cascade dial rule, if you select **General VaaS Service as the Dial string matching format** and also select one of the SIP options as the **Dial type**, content sharing during conferences may not work.

Procedure

1. Go to **Service Config > Dial Plan > Dial Plans**.
2. Select the dial plan used for H.323 and SIP signaling.
3. In **Dial Rules**, select the **Add** button to add a new dial rule.
4. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a brief description of the dial rule.</td>
</tr>
<tr>
<td>Action</td>
<td>Select <strong>Resolve to conference room with autodial</strong>.</td>
</tr>
<tr>
<td>Relay Media</td>
<td>Select this option only if you’re adding the dial rule to a RealPresence DMA combination-configured system.</td>
</tr>
<tr>
<td>Conference template</td>
<td>Select the check box, then choose a conference template. If you don’t select this option, the system uses the default conference template specified in Conference Settings.</td>
</tr>
</tbody>
</table>
| MCU pool order      | When checked, choose the MCU pool order to use for MCUs that provide auto dial-out cascade functionality.  
                      | If you select a specific MCU pool order, you must H.323 register each MCU in the pool with the RealPresence DMA system.  
<pre><code>                  | If you leave this option unchecked, the dial rule uses the default pool order selected in Conference Settings. |
</code></pre>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU affinity</td>
<td>When checked, choose the MCU affinity as follows:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>Prefer MCU in first MCU pool</strong></td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system routes the call to the first available MCU in the default MCU pool order.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option and also choose a specific <strong>MCU pool order</strong>, the RealPresence DMA system selects an MCU from that pool order.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>Prefer MCU in first caller’s site</strong></td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system routes the call to an MCU from the same site as the first caller if that MCU is part of the MCU pool in the default pool order. Note that Internet calling must be enabled from the site.</td>
</tr>
<tr>
<td></td>
<td>If you choose this option and also choose a specific <strong>MCU pool order</strong>, the RealPresence DMA system selects an MCU from that pool order.</td>
</tr>
<tr>
<td></td>
<td>When not checked, MCU affinity defaults to the value selected in Conference Settings.</td>
</tr>
<tr>
<td>Autodial name</td>
<td>The name assigned to signaling for the auto dial-out cascade link. The VaaS provider displays this as the name of the participant dialing in.</td>
</tr>
<tr>
<td></td>
<td>You can use the default autodial name or enter a new name as needed.</td>
</tr>
<tr>
<td>Preliminary</td>
<td>Select the check box to enter preliminary script options for matching the dial string.</td>
</tr>
<tr>
<td>Dial string matching format</td>
<td>Field is active only if you select the <strong>Preliminary</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>Select the dial string format to match for the type of cascade dial-out:</td>
</tr>
<tr>
<td></td>
<td>•  <strong>RealConnect for Teams</strong> - Microsoft Teams conferences.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>General VaaS Service</strong> - Any cloud-based Video as a Service conference with the dial string format conferenceid@domain or userid@domain.</td>
</tr>
<tr>
<td></td>
<td>•  <strong>Custom</strong> - Enter a customized script in the <strong>Use customized script</strong> field or in the <strong>Preliminary</strong> tab.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tenant ID format</td>
<td>Field displays only if you select the Preliminary check box and RealConnect for Teams as the dial string matching format. Enter a specific tenant ID format to match, or leave the default value to match any tenant ID format. An example of a tenant ID format is the format of the tenant ID assigned to your VaaS subscription service.</td>
</tr>
<tr>
<td>Conference/User ID format</td>
<td>Field is active on both the Dial Rule and Preliminary tabs when you select the Preliminary check box and RealConnect for Teams or General Vaas Service as the dial string matching format. Leave the default value to match to any conference or user ID format or enter a specific conference/user ID format to match.</td>
</tr>
<tr>
<td>Domain format</td>
<td>Field is active on both the Dial Rule and Preliminary tabs when you select the Preliminary check box and RealConnect for Teams or General Vaas Service as the dial string matching format. Leave the default value to match to any conference or user ID@domain format or enter a specific domain to match (for example, enter .*vc for MS Teams conferences). It's recommended that you enter a specific domain (for example, .*vc for MS Teams conferences) to prevent calls other than auto dial-out cascade calls from matching the default filter.</td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial type</td>
<td>Defines the signaling protocol and method used to perform the cascade dial-out. All dial-outs point to the RealPresence DMA edge system or RealPresence Access Director system.</td>
</tr>
<tr>
<td></td>
<td>• If you select RealConnect for Teams as the Dial string matching format, you must choose External gatekeeper or URI by Site Topology for H.323 as the Dial type.</td>
</tr>
<tr>
<td></td>
<td>• If you select General VaaS Service as the Dial string matching format and also select one of the SIP options as the Dial type, content sharing during conferences may not work.</td>
</tr>
<tr>
<td></td>
<td><strong>External Gatekeeper</strong> – if selected, use the configured gatekeepers and send the dial-out statically to them as an H.323 call.</td>
</tr>
<tr>
<td></td>
<td><strong>SIP Peer</strong> – if selected, use the configured SIP peers and send the dial-out statically to them as a SIP call.</td>
</tr>
<tr>
<td></td>
<td><strong>URI by Site Topology for H.323</strong> – Uses site topology H.323 settings to determine the next-hop destination for the H.323 dial-out (the next-hop is generally a RealPresence DMA edge system).</td>
</tr>
<tr>
<td></td>
<td><strong>URI by Site Topology for SIP</strong> – Uses site topology SIP settings to determine the next-hop destination for the SIP dial-out (the next-hop is generally a RealPresence DMA edge system).</td>
</tr>
<tr>
<td></td>
<td><strong>URI by Site Topology for SIPS</strong> – Uses site topology SIPS settings to determine the next-hop destination for the secure SIPS dial-out (the next-hop is generally a RealPresence DMA edge system).</td>
</tr>
</tbody>
</table>

5. Select the **Preliminary** tab and enter a preliminary script if needed (optional).

   If you selected **Custom** as the **Dial string matching format**, you can add a preliminary script in the **Use customized script** field or go to the **Preliminary** tab to add larger scripts.

6. Select **OK** to save the dial rule.

### Add a Dial Rule for Auto Dial-out Cascading to MS Teams Conferences Using the Teams Conference ID

When you use a custom preliminary script, you can simplify dialing into Microsoft Teams conferences by requiring that callers dial only the Microsoft Teams conference ID to join a conference.

The preliminary script in the following steps contains six editable variables, noted with a comment that begins with // EDIT:. The script also has code to support unregistered endpoints (H.323 and SIP) that call into a Microsoft Teams conference. You can remove this part of the script if necessary; if you leave it in, you don’t need to use additional scripts to allow unregistered endpoints (see Calls from Unregistered Endpoints to Cloud Service-based Conferences).
The additional dial rule must come after the auto dial-out cascade dial rule for registered users in the dial plan.

Procedure
1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan used for H.323 and SIP signaling.
3. Under Dial Rules, click the Add button to add a new dial rule.
4. In the Action field, select Resolve to conference room with autodial.
5. In the Dial string matching format field, select Custom.
6. Select the Preliminary tab and enter the following script in the Use customized script text box:

```javascript
//-------------------------------------------
// RealConnect for Teams Preliminary Script
//
// This preliminary script supports the RealConnect for Teams feature
// by allowing the user to dial the Teams conference
// with the following criteria:
//
//  1) Conference ID format (<conferenceID> or
//     <conferenceID>@<domain> or full conference format
//     (<tenantID>.<conferenceID>[@<domain>])
//  2) H.323 or SIP
//  3) Registered or unregistered endpoints (For unregistered
//     endpoints, configure the Call Server Settings to allow calls
//     from unregistered endpoints.)
//
// To use this script, edit the variables that are commented with the
// word 'EDIT' to match your Teams site requirements.
// After editing, copy and paste the script into the Preliminary
// script area of the 'Resolve to conference room with autodial' dial
// rule.

```

```javascript
// <-- Copy the lines below here and paste into the Preliminary
// script area of the 'Resolve to conference room with autodial' dial
// rule -->

```

```javascript
//-------------------------------------------
// User Configurable Values - Start
//-------------------------------------------
//
// These three variables are for Teams conference calls with only the
// conference ID in the dial string. Edit the value of these
// variables
// to match your site requirements.
//
// EDIT: The length of the conference IDs assigned to your tenant ID
// var conferenceIDLength = 9;
// EDIT: The Teams tenant ID assigned to your subscription
// var tenantID = '888888';
// EDIT: The domain assigned to your Teams tenant.
// var domainID = 't.plcm.vc';

```

```javascript
// These three variables are for processing the full Teams conference
// with autodial dial string "<tenant id>.<conference id>@<domain>"
// Customize them for your site or leave them as the defaults. These
```
// values are javascript regex strings. The default values provided
// will accept any value with the correct format.

// EDIT: The Teams tenant ID assigned to your subscription or a regex
// that
// encompasses the list of tenant IDs.
var tenantIdMatchStr = '[^:#*.*]+';
// EDIT: A regex that encompasses the list of conference IDs possible
// for
// your site.
var roomIdMatchStr = '[^:#*.*]+';
// EDIT: The domain for your subscription or a regex that encompasses
// the
// list of domains.
var domainMatchStr = '.*vc';

// Please use the "Debug this Script" tool to verify that the changes
to
// the values are working as expected.
// User Configurable Values - End

DIAL_STRING = processDialString(DIAL_STRING);

if (DIAL_STRING === 'REJECT')
{
    return NEXT_RULE;
}

// Main function

function processDialString(dialString)
{
    dialString = checkForConferenceOnly(dialString);

    if (dialString.indexOf('@') != -1 && !matchesDialPatterns(dialString))
    {
        // For unregistered users dialing the full Teams string, the
domain may not match the pattern. Replace it
        // with the specified Conference ID-only 'domainID' and try
        again to see if it's a match.
        dialString = transformUnregisteredDialString(dialString);
    }

    if (!matchesDialPatterns(dialString))
    {
        return 'REJECT';
    }

    return dialString;
}

// Supporting functions

Dial Plans

325
function transformUnregisteredDialString(dialString) {
  var domainPart='@' + domainID;
  var matchPattern = '\s*(sip:|sips:|[hH]323:)\s*(autodial-|partadial-)?\s*\s*\s*' + tenantID + '\s*.*$';
  if (dialString.match(matchPattern)) {
    if (dialString.indexOf('@') == -1) {
      dialString = dialString + domainPart;
    } else {
      dialString = dialString.replace(/(^([^@]*))@(.*)/i, "$1" + domainPart);
    }
  }
  return dialString;
}

function matchesDialPatterns(dialString) {
  var atPattern = '\s*(sip:|sips:|[hH]323:)\s*(autodial-|partadial-)?\s*\s*\s*' + tenantIdMatchStr + '\[*\].' + roomIdMatchStr + '@\s*\s*\s*\s*\s*$';
  var specialDialPattern = '\s*(sip:|sips:|[hH]323:)\s*(autodial-|partadial-).*';
  var poundPattern = '\s*\[#]*\s*' + domainMatchStr + '\[#\]{' + 2 + '}\s*\s*\s*\s*\s*$';
  if (!isMatch(atPattern, dialString) && !isMatch(specialDialPattern, dialString) && !isMatch(poundPattern, dialString)) {
    return false;
  }
  return true;
}

function isMatch(pattern, stringToMatch) {
  return (stringToMatch.match(pattern) !== null);
}

function checkForConferenceOnly(dialString) {
  var indexOfDot = dialString.indexOf('.');
  var indexOfAt = dialString.indexOf('@');
  var matchConferenceIdOnlyPattern = '\s*(sip:|sips:|[hH]323:)\s*' + conferenceIDLength + '\s*\s*\s*\s*\s*$';
  var atConferenceIdOnlyPattern = '\s*(sip:|sips:|[hH]323:)\s*\s*\s*\s*\s*\s*\s*$';
  var poundConferenceIdOnlyPattern = '\s*\[#]*\s*' + domainMatchStr + '\[#\]{' + conferenceIDLength + '}\s*\s*\s*\s*\s*$';
  if (indexOfDot == -1 && indexOfAt == -1 && dialString.match(matchConferenceIdOnlyPattern)) {
    return true;
  }
  return false;
}
```javascript
function transformDialString(dialString) {
    var dotPart = '.';
    var domainPart = '@' + domainID; // The domain assigned to your Teams tenant.
    var matchPattern = '\s*(sip:|sips:|[hH]323:)?\s*\d{10}\s*.*$';
    var atPattern = '\s*(sip:|sips:|[hH]323:)?\s*\d{10}@[^:#*]+\s*[:;]?.*$';
    var prefixPart = '';  
    var conferenceID = dialString;
    var indexOfColon = dialString.indexOf(':');
    var indexOfAt = dialString.indexOf('@');

    if (dialString.match(atPattern)) {
        if (indexOfColon != -1) {
            prefixPart = dialString.substring(0, indexOfColon + 1);
            conferenceID = dialString.substring(indexOfColon + 1, indexOfAt);
        } else {
            conferenceID = dialString.substring(0, indexOfAt);
        }
        if (conferenceID.length == conferenceIDLength) {
            dialString = prefixPart + tenantID + dotPart + conferenceID + domainPart;
        }
    } else if (dialString.match(matchPattern)) {
        if (indexOfColon != -1) {
            prefixPart = dialString.substr(0, indexOfColon + 1);
            conferenceID = dialString.substr(indexOfColon + 1);
        }
        if (conferenceID.length == conferenceIDLength) {
            dialString = prefixPart + tenantID + dotPart + conferenceID + domainPart;
        }
    }
    return dialString;
}
```
dialString = prefixPart + tenantID + dotPart + conferenceID + domainPart;
}
}
return dialString;

7. In the script, customize the values of the variables in the User Configurable Values section.

8. Click Debug this Script to verify that the dial string is transformed correctly in the following format:

   `<tenant ID>.<conference ID>@<domain>`

   For example, `000000.123456789@t.plcm.vc`.

9. Click OK to save the dial rule.

10. In the list of dial rules, move the rule so that it follows the auto dial-out cascade dial rule for registered users.

11. Click Test Dial Plan to ensure that the dial rule is working within the dial plan as expected.

### Allowing Calls from Unregistered Endpoints to Cloud Service-based Conferences

Some unregistered H.323 endpoints remove domain information from the dial string when calling into Microsoft Teams or other cloud service-based conferences, which causes calls to fail. You can add auto dial-out cascade dial rules to prevent the call failures.

Two options are available to prevent calls from failing when unregistered H.323 endpoints remove domain information from the dial string:

- Add an auto dial-out cascade dial rule that allows only SIP endpoints to make unregistered calls to cloud-based conferences.
- Add an auto dial-out cascade dial rule that allows calls from unregistered H.323 endpoints by adding domain details back to the dial string.

### Add an Auto Dial-Out Cascade Dial Rule to Allow Only SIP Endpoints to Make Unregistered Calls to Cloud-Based Conferences

An auto dial-out cascade dial rule can be added to a dial plan to allow only SIP endpoints to make unregistered calls to cloud service-based conferences.

Some unregistered H.323 endpoints remove domain information from the dial string when calling into cloud-based conferences, which causes calls to fail. To prevent the call failures, you can add a custom auto dial-out cascade dial rule that allows only SIP endpoints to make unregistered calls to cloud-based conferences.

**Procedure**

1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan used for H.323 and SIP signaling.
3. Under Dial Rules, click the Add button to add a new dial rule.
4. In the Action field, select Resolve to conference room with autodial.
5. In the Dial string matching format field, select Custom.
6. Add a line to the preliminary script to replace the domain information of the call from the unregistered endpoint with the domain of the VaaS provider or Microsoft Teams domain.
Dial Plans

The following example is for a Microsoft Teams domain:
DIAL_STRING = DIAL_STRING.replace(/^([^@]*)@(.*)/i,"$1<@domain>"); //
Enter your own Teams domain for <@domain> e.g. "@t.plcm.vc"
7. Click OK to add the dial rule.
8. In the list of dial rules, move the rule so that it follows the auto dial-out cascade dial rule for
registered users.

Add an Auto Dial-out Cascade Dial Rule to Allow Calls from Unregistered H.323
Endpoints to Cloud-Based Conferences
You can add an auto dial-out cascade dial rule to a dial plan to allow unregistered H.323 endpoints to call
cloud service-based conferences.
Some unregistered H.323 endpoints remove domain information from the dial string when calling into
cloud service-based conferences, which causes calls to fail. To enable these calls to complete, you can
add an additional auto dial-out cascade dial rule that will add domain information back to the dial string by
using a custom preliminary script.
The additional dial rule must come after the auto dial-out cascade dial rule for registered users in the dial
plan.
Procedure
1. Go to Service Config > Dial Plan > Dial Plans.
2. Select the dial plan used for H.323 and SIP signaling.
3. Add a dial rule as described in Add a Dial Rule for Auto Dial-out Cascading to a Cloud Servicebased Conference.
4. In the Dial string matching format field, select Custom.
5. In the Use customized script field, add a preliminary script similar to the following script (revise
as needed for your videoconferencing environment):
// This is an example script for demonstration purposes. You will
need to tailor this script to your environment.
// For Teams conference calls, the dial string format must be in the
format “<tenant>.<conference>@<domain>”. Not all VaaS conferences
require a tenant ID but Teams conferences do.
// For unregistered callers, some H.323 devices are removing the
“@domain” portion of the dial sting when
// the call is established. Without that domain information, the
call will fail. Add the domain part of
// the dial string back if necessary.
var tenant="000000"; // Enter your own tenant ID here
var domainPart="@t.plcm.vc"; // Enter your Teams domain here
var matchPattern = '\s*(sip:|sips:|[hH]323:)?\s*(autodial-|
partadial-)?' + tenant + '\s*.*$';
if (DIAL_STRING.match(matchPattern))
{
if (DIAL_STRING.indexOf('@') == -1)
{
DIAL_STRING = DIAL_STRING + domainPart;
}
else
{
DIAL_STRING = DIAL_STRING.replace(/^([^@]*)@(.*)/i,"$1" +

329


domainPart);
}

else
{
    return NEXT_RULE;
}

6. Click OK to add the dial rule.
7. In the list of dial rules, move the rule so that it follows the auto dial-out cascade dial rule for registered users.

Prevent an MCU from Playing Audio Announcements During an Auto Dial-out Cascade Conference

Participants in a dial-out cascade conference may hear RealPresence Collaboration Server audio announcements such as the "Welcome" message.

You can prevent the audio files from being played by configuring certain settings on the MCUs and the RealPresence DMA system.

If you have more than one dial rule with the action to Resolve to conference room with autodial, you need to edit each dial rule to use the new conference template you create in the following steps.

Procedure
1. From the RMX Manager, create a new IVR service on each MCU to be used for the auto dial-out cascade link to a VaaS-based conference.
2. Configure the settings on the tabs as follows:
   - Welcome – clear the Enable Welcome Message check box.
   - Conference Chairperson – clear the Enable Chairperson Messages check box.
   - Conference Password – clear the Enable Password Messages check box.
   - Roll Call/Notifications – clear the Enable Roll Call check box.
   - Operator Assistance – clear the Enable Operator Assistance check box.
   - General – for each file action name, select the empty option at the top of the message file drop-down box.
3. On the RealPresence DMA system, go to Service Config > Conference Templates and add a new conference template.
4. Configure the following settings:
   - Polycom MCU Conference IVR – select the Override default conference IVR service check box.
   - Conference IVR service – select the conference IVR service that you created on the MCU(s).
5. Go to Service Config > Dial Plan > Dial Plans.
6. Select the Resolve to conference room with autodial dial rule.
7. Select the Edit button.
8. Select the Conference template check box.
9. Select the new conference template you created.
10. Test a dial-out cascade conference to ensure that audio messages can’t be heard by participants.
Associating a Dial Plan to a Call Service
You can associate a dial plan with each call service you have enabled for your call server. You can also assign a dial plan for both authorized and unauthorized (guest port) calls.

Associate a Dial Plan to SIP Service
In SIP Settings, you can select a dial plan to associate with both unencrypted and TLS ports.

Procedure
1. Go to Service Config > SIP Settings.
2. Under Authorized ports, use the Dial plan drop-down list to select a dial plan for both the Unencrypted SIP port and TLS port.
3. Click Update to save your settings.

Associate a Dial Plan to H.323 Service
In H.323 Settings, you can select a dial plan to associate with.

Procedure
1. Go to Service Config > H.323 Settings.
2. Select the dial plan to apply to H.323 calls.
3. Click Update to save your settings.

Associate a Dial Plan to WebRTC Service
In WebRTC Settings, you can select a dial plan for both authorized and unauthorized WebRTC calls.

Procedure
1. Go to Service Config > WebRTC Settings.
2. Select the Authorized Dial plan and Unauthorized Dial plan to apply to WebRTC calls.
3. Click Update to save your settings.

Test a Dial Plan
You can specify various caller parameters and a dial string, and see how each dial rule handles such a call and what its final disposition is.

Procedure
1. Go to Service Config > Dial Plan > Dial Plans.
2. In the Dial Plan list, select a dial plan to test and click Test Dial Plan.
3. Complete the fields in the following table as required.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial string</td>
<td>Enter a dial string to test. Then click <strong>Test</strong>. For SIP, the dial string should always specify the schema prefix (sip or sips). For example: sips:rbruce@10.47.7.9</td>
</tr>
<tr>
<td>Caller site</td>
<td>Select a site in order to set the four caller site variables:</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>CALLER_SITE_NAME</strong></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>CALLER_SITE_DIGITS</strong></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>CALLER_SITE_COUNTRY_CODE</strong></td>
</tr>
<tr>
<td></td>
<td>▪ <strong>CALLER_SITE_AREA_CODE</strong></td>
</tr>
<tr>
<td></td>
<td>These variables can’t be set directly and are display only.</td>
</tr>
<tr>
<td>CALLER_H323ID</td>
<td>Test caller's H.323 ID or blank.</td>
</tr>
<tr>
<td>CALLER_E164</td>
<td>Test caller's H.323 E.164 alias or blank.</td>
</tr>
<tr>
<td>CALLER_TEL_URI</td>
<td>Test caller’s SIP tel URI or blank.</td>
</tr>
<tr>
<td>CALLER_SIP_URI</td>
<td>Test caller’s SIP sip URI or blank.</td>
</tr>
<tr>
<td>VMR/Skype Conf ID</td>
<td>This field specifies the return value of the function getConferenceRoomOrID(), and is only populated when the dial rule simulates an outbound call to an endpoint from a conference based on a VMR or Skype conference ID. If the dial rule simulates a call to a VMR or Skype conference ID or a dial-in call, this field is blank.</td>
</tr>
<tr>
<td>Test route output</td>
<td>Displays the results of applying each rule (including it's preliminary, if any) to the dial string. For instance, testing the dial string example shown above against the default dial plan might result in the following: #1: SipAlias[sips:rbruce@10.47.7.9] is not registered. H323-ID[rbruce] is not registered. #2: The room [rbruce] does not exist. #3: No entry queue is found. #4: Domain [10.47.7.9] is not within our administration. #5: The call was accepted by this dial rule.</td>
</tr>
<tr>
<td>Final result</td>
<td>Displays the final outcome of the dial rule processing. The final outcome for the example above would be: Transformed dial string is [sips:rbruce@10.47.7.9]. The call was accepted by dial rule #5.</td>
</tr>
</tbody>
</table>

4. **Complete the required fields and click Test.**
Prefix Service

Topics:

- Add Simplified ISDN Gateway Dialing Prefix
- Edit Simplified ISDN Gateway Dialing Prefix
- Edit Vertical Service Code

The Prefix Service list provides all configured prefixes in one place so you can determine what prefixes are in use and whether any conflicts exist.

You can perform the following actions on a service or device with a prefix:

- Add, edit, or delete any of the devices without having to navigate back to the specific page for that device type. Devices include an external gatekeeper, external SIP peer, external H.323 SBC, and MCU.
- Add, edit, or delete simplified ISDN gateway dialing services.
- Edit the name, vertical service code, or description of the forwarding and hunt group services and enable or disable them.

The following table describes the fields in the list:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service/Device name</td>
<td>The name of the service or device assigned the specified prefix(es). Devices with no prefix(es) assigned are listed, but shown as disabled.</td>
</tr>
<tr>
<td>Prefix range</td>
<td>The dial string prefix(es) assigned to this service or device.</td>
</tr>
<tr>
<td>Service/Device type</td>
<td>Type of service or device.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service or device.</td>
</tr>
<tr>
<td>Service status</td>
<td>Indicates whether the service or device is enabled or disabled.</td>
</tr>
</tbody>
</table>

Add Simplified ISDN Gateway Dialing Prefix

You can create a new prefix-driven simplified ISDN gateway dialing service for using external ISDN gateways.

This feature is not related to the RealPresence DMA system’s built-in H.323 <-> SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways.

This feature is not supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix.

Procedure

1. Go to Service Config > Dial Plan > Prefix Service.
2. Click Add Simplified ISDN Gateway Dialing.
3. Complete the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Simplified ISDN dialing prefix</td>
<td>The dial string prefix(es) assigned to this service.</td>
</tr>
<tr>
<td></td>
<td>Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes</td>
</tr>
<tr>
<td></td>
<td>separated by commas (44,46), or a combination (41, 44-47, 49).</td>
</tr>
<tr>
<td></td>
<td>If your dial plan uses the <strong>Dial services by prefix</strong> dial rule (in the</td>
</tr>
<tr>
<td></td>
<td>default dial plan) to route calls to services, all dial strings beginning</td>
</tr>
<tr>
<td></td>
<td>with an assigned prefix are forwarded to this service for resolution.</td>
</tr>
<tr>
<td>Use all ISDN gateways</td>
<td>Indicates whether this service applies to all available gateways or only</td>
</tr>
<tr>
<td></td>
<td>those selected below.</td>
</tr>
<tr>
<td>Available ISDN gateways</td>
<td>Lists the ISDN gateways that have at least one session profile specifying</td>
</tr>
<tr>
<td></td>
<td>an H.320 or PSTN protocol.</td>
</tr>
<tr>
<td>Selected ISDN gateways</td>
<td>Lists the selected ISDN gateways.</td>
</tr>
<tr>
<td></td>
<td>The arrow buttons move gateways from one list to the other.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

### Edit Simplified ISDN Gateway Dialing Prefix

You can edit a prefix-driven simplified ISDN gateway dialing service.

**Note:** This feature is not related to the RealPresence DMA system's built-in H.323<->SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways. This feature isn't supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix.

**Procedure**

1. Go to Service Config > Dial Plan > Prefix Service.
2. Select a **Simplified ISDN Gateway Dialing** service and click **Edit**.
3. Revise the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Simplified ISDN dialing prefix</td>
<td>The dial string prefix(es) assigned to this service. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44, 46), or a combination (41, 44-47, 49). If your dial plan uses the <strong>Dial services by prefix</strong> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this service for resolution.</td>
</tr>
<tr>
<td>Use all ISDN gateways</td>
<td>Indicates whether this service applies to all available gateways or only those selected below.</td>
</tr>
<tr>
<td>Available ISDN gateways</td>
<td>Lists the gateways that have at least one session profile specifying an H.320 or PSTN protocol.</td>
</tr>
<tr>
<td>Selected ISDN gateways</td>
<td>Lists the selected gateways. The arrow buttons move gateways from one list to the other.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Edit Vertical Service Code**

You can edit a call forwarding or hunt group service invoked when callers dial the vertical service code (VSC) for that service, followed by the alias. These services are included on the **Prefix Service** page and cannot be deleted, but you can disable them or change their names, descriptions, or VSCs. If you change the VSCs, be sure to inform users of the change.

**Procedure**

1. Go to **Service Config > Dial Plan > Prefix Service**.
2. Select a service or device with a vertical service code.
3. Click **Edit**.
4. Revise the fields in the following table as required:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of service. This field cannot be edited.</td>
</tr>
<tr>
<td>Name</td>
<td>A display name for this service.</td>
</tr>
<tr>
<td>Code</td>
<td>The vertical service code (VSC) for this service. Must consist of an asterisk/star (*) followed by two digits. Registered endpoints can activate this feature by dialing the VSC followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Clearing this check box turns off the service.</td>
</tr>
</tbody>
</table>
5. Click **OK**.
Hunt Groups

Topics:
- Add a Hunt Group
- Edit a Hunt Group
- Add an Alias
- Edit an Alias

A hunt group is a set of endpoints that share an alias or aliases.

Hunt groups can be used to define a dial string shared by a group of people, such as a technical support number. When the RealPresence DMA system call server resolves a dial string to the hunt group's alias, it selects a member of the group and tries to terminate the call to that member.

The system selects hunt group members in round-robin fashion. It skips members that are in a call or have unconditional call forwarding enabled. If the selected group member rejects the call or doesn't answer before the timeout, the system tries the next group member.

If all members have been attempted (or skipped) without successfully terminating the call, the system sends a busy message to the caller.

Registered endpoints can add themselves to a hunt group by dialing the vertical service code (VSC) for joining (default is *71) followed by the hunt group alias. They can leave a hunt group by dialing the VSC for leaving (default is *72) followed by the hunt group alias. An endpoint can belong to multiple hunt groups.

Add a Hunt Group

You can define a new hunt group in the system and add members to it.

Procedure
1. Go to Service Config > Dial Plan > Hunt Groups.
2. Select the Add button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Hunt group name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the Hunt Groups list.</td>
</tr>
<tr>
<td>No answer timeout (seconds)</td>
<td>Number of seconds to wait for a hunt group member to answer a call before giving up and trying another member.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Aliases</td>
<td>Lists the aliases (dial strings) that resolve to this hunt group. Click <strong>Add</strong> to add an alias. Click <strong>Edit</strong> or <strong>Delete</strong> to change or remove the selected alias.</td>
</tr>
</tbody>
</table>

**Hunt Group Members**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Search for endpoints by alias, IP address, or registration status.</td>
</tr>
<tr>
<td>Available</td>
<td>Lists the endpoints that match the search criteria.</td>
</tr>
<tr>
<td>Member</td>
<td>Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.</td>
</tr>
</tbody>
</table>

4. **Click OK.**

**Edit a Hunt Group**

You can modify the selected hunt group and add or remove members.

**Procedure**

1. Go to **Service Config > Dial Plan > Hunt Groups.**
2. Select the hunt group of interest and click **Add.**
   - The **Edit Hunt Group** dialog displays.
3. Revise the fields as described in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Hunt group name.</td>
</tr>
<tr>
<td>Description</td>
<td>The text description displayed in the <strong>Hunt Groups</strong> list.</td>
</tr>
<tr>
<td>No answer</td>
<td>Number of seconds to wait for a hunt group member to answer a call before giving up and trying another member.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Lists the aliases (dial strings) that resolve to this hunt group. Click <strong>Add</strong> to add an alias. Click <strong>Edit</strong> or <strong>Delete</strong> to change or remove the selected alias.</td>
</tr>
</tbody>
</table>

**Hunt Group Members**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Search for endpoints by alias, IP address, or registration status.</td>
</tr>
<tr>
<td>Available</td>
<td>Lists the endpoints that match the search criteria.</td>
</tr>
<tr>
<td>Member</td>
<td>Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.</td>
</tr>
</tbody>
</table>
4. Complete the required fields and click OK.

Add an Alias
You can add an alias value to the hunt group.

Procedure
1. Go to Service Config > Dial Plan > Hunt Groups.
2. In the Actions list click Add.
   The Add Hunt Group dialog appears.
3. Under the Alias Type list, click Add.
   Aliases should be specified by their fully qualified dial string. For example, to specify that H.323 callers can call the hunt group by dialing 1234, enter 1234. To specify that SIP callers can call the hunt group by dialing 1234, enter sip:1234@mydomain.com.
4. Fill in the Value field in the Add Alias dialog and click OK.

Edit an Alias
You can change an alias value assigned to the hunt group.

Procedure
1. Go to Service Config > Dial Plan > Hunt Groups.
2. In the Actions list click Edit.
   The Edit Hunt Group dialog appears.
3. Under the Alias Type list, click Edit.
   Aliases should be specified by their fully qualified dial string. For example, to specify that H.323 callers can call the hunt group by dialing 1234, enter 1234. To specify that SIP callers can call the hunt group by dialing 1234, enter sip:1234@mydomain.com.
4. Fill in the Value field in the Edit Alias dialog and click OK.
Domains Restrictions

Topics:

- Add a Local Domain
- Remove a Local Domain
- Restore Defaults

On the Domain Restrictions page, you can add administrative domains to or remove them from the list of domains from which registrations are accepted.

If the local domain list is empty, all domains are considered local, and the system accepts endpoint registrations from any domain. Otherwise, it accepts registrations only from the listed domains. This is a supercluster-wide configuration.

Calls that have a non-local domain in the dialed string don’t resolve to any locally registered endpoints, and can only resolve to a VEQ or VMR if the Conference rooms belong to every domain check box is checked.

Note: The Resolve to external address dial rule action doesn’t match against domains that are considered local. If the list of domains is empty and all domains are considered local, this dial rule action doesn’t match any dial string and can’t be used. In some circumstances (depending on network topology and configuration), dialing loops can develop if you don’t restrict the RealPresence DMA system to specific domains.

Add a Local Domain

You can add a local domain to the system.

IP addresses, including IP addresses with the wildcard character, and domain names are accepted.

Domain names must be full domains, but you can replace a single host label within a domain with the wildcard character to match multiple sub-domains. For example, *.mycompany.com matches:

- eng.mycompany.com
- fin.mycompany.com

And eng.*.mycompany.com matches:

- eng.sanjose.mycompany.com
- eng.austin.mycompany.com

Sub-domains are not local if the domain is listed without a wildcard character.

For example, if the domain mycompany.com is entered without any other mycompany domains, this would NOT match eng.mycompany.com.

Procedure

1. Go to Service Config > Dial Plan > Domain Restrictions.
2. In the Add new local domain field, enter a domain and click Add.

The system adds the domain to the Local domains list.
3. Configure the settings described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally registered SIP endpoints belong to every local domain</td>
<td>Specifies that call requests for locally registered SIP endpoints don't have to match the domain. For example, if there's an endpoint registered as sip:johnsmith@1.1.1.1 and this option is enabled, a call to sip:<a href="mailto:johnsmith@mycompany.com">johnsmith@mycompany.com</a> may be connected to that endpoint. If this option is not selected, call requests must exactly match the URI of the registered endpoint.</td>
</tr>
<tr>
<td>Email IDs of registered H.323 endpoints belong to every local domain</td>
<td>Specifies that call requests for locally registered H.323 endpoint email IDs don't have to match the domain. For example, if there's an endpoint registered as :johnsmith@1.1.1.1 and this option is enabled, a call to <a href="mailto:johnsmith@mycompany.com">johnsmith@mycompany.com</a> may be connected to that endpoint. If this option is not selected, call requests must exactly match the URI of the registered endpoint.</td>
</tr>
<tr>
<td>Conference rooms, virtual entry queues and RealConnect conferences belong to every domain</td>
<td>Specifies that if the dial string identifies a conference room (VMR), virtual entry queue (VEQ), or Skype for Business conference ID on the RealPresence DMA system and includes a domain, a dial rule implementing the Resolve to conference room ID, Resolve to virtual entry queue, or Resolve to conference ID by Skype query actions ignores the domain and routes the call to that conference room, VEQ, or conference ID. If this option is not selected, a dial string's domain must be a local domain for the system to route the call to a conference room, VEQ, or conference ID.</td>
</tr>
</tbody>
</table>

4. Click Update.

**Remove a Local Domain**

You can remove a local domain from the system.

**Procedure**

1. Go to Service Config > Dial Plan > Domain Restrictions.
2. In the Local domains list, select a domain and click Remove.
3. Click Update.

**Restore Defaults**

When you restore defaults, all domains are removed so that the system accepts registrations from any domain.
Procedure

1. Go to Service Config > Dial Plan > Domain Restrictions.
2. Click Restore Defaults to remove all domains.
3. Click Update.
Preliminary and Postliminary Scripting

Topics:
- Predefined Preliminary/Postliminary Scripting Variables
- Preliminary/Postliminary Scripting Functions
- How Dial Rule Actions Affect SIP Headers
- Test Preliminary and Postliminary Scripts
- Sample Preliminary and Postliminary Scripts

A preliminary is an executable script, written in the JavaScript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule's action is performed.

A postliminary is an executable script, written in the JavaScript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the DIAL_STRING variable (initially this is set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule's action (if the filter criteria isn't met) or return one of the following:
- **NEXT_RULE**: Skips the rule being processed and passes the dial string to the next rule
- **BLOCK**: Rejects the call

### Predefined Preliminary/Postliminary Scripting Variables

The following table describes the predefined variables you can use in a preliminary or postliminary script. The script can evaluate a variable or change its value (the change isn't preserved after the script completes).

<table>
<thead>
<tr>
<th>Variable</th>
<th>Initial value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALLER_E164</td>
<td>For H.323 calls only, an array variable initially set to the set of E.164 addresses of the caller. The length of the array is 0 if the caller doesn't have an E.164 address.</td>
</tr>
<tr>
<td>CALLER_H323ID</td>
<td>Array variable initially set to the set of H323ID addresses of the caller. The length of the array is 0 if the caller doesn't have an H323ID address.</td>
</tr>
<tr>
<td>CALLER_IS_IPV6</td>
<td>TRUE if the caller is an IPv6 endpoint. Blank otherwise.</td>
</tr>
<tr>
<td>CALLER_SIP_URI</td>
<td>Array variable initially set to the set of SIP URI addresses of the caller. The length of the array is 0 if the caller doesn't have a SIP URI address.</td>
</tr>
<tr>
<td>CALLER_SITE_AREA_CODE</td>
<td>Area code of the caller's site. Blank if the site doesn't have an area code.</td>
</tr>
<tr>
<td>Variable</td>
<td>Initial value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CALLER_SITE_COUNTRY_CODE</td>
<td>Country code of the caller's site. Blank if the site doesn't have a country code.</td>
</tr>
<tr>
<td>CALLER_SITE_DIGITS</td>
<td>The number of subscriber number digits in the caller's site (that is, the length of a phone number at the site, excluding area code). Blank if the site doesn't have a number of digits.</td>
</tr>
<tr>
<td>CALLER_SITE_NAME</td>
<td>The name of the caller's site.</td>
</tr>
<tr>
<td>CALLER_TEL_URI</td>
<td>Array variable initially set to the set of Tel URI addresses of the caller. The length of the array is 0 if the caller doesn't have a Tel URI address.</td>
</tr>
</tbody>
</table>
| DIAL_STRING                  | Initially set to the dial string being evaluated. If the script modifies the DIAL_STRING value, the modified value is used as the input to the dial rule action.  
For SIP, when the DIAL_STRING is modified by the script, its use depends on the dial rule action: |
| INPUT_SIP_HEADERS            | For SIP calls only, an associative array containing the SIP headers in the received SIP INVITE message.  
Usage example:  
```java  
if(INPUT_SIP_HEADERS["Supported"].matches(/.*ms-forking.*))  
{  
  ...  
}  ``` |
Variable | Initial value
--- | ---
OUTPUT_SIP_HEADERS | An empty associative array. Headers that the script adds to this array replace the corresponding headers in the received SIP INVITE message. If a header added to this array isn't in the received INVITE message, it's added to the INVITE message.

**Usage example 1:**

```java
var list = OUTPUT_SIP_HEADERS.get("User-Agent");
if (list == null)
{
    list = new java.util.LinkedList();
    OUTPUT_SIP_HEADERS.put("User-Agent", list);
}
list.add("Someone. Not a RealPresence DMA 7000.");
```

**Usage example 2:**

```java
var list = OUTPUT_SIP_HEADERS.get("Some-Custom-Header");
if (list == null)
{
    OUTPUT_SIP_HEADERS.put("Some-Custom-Header", list);
}
list.add("Whatever you want");
```

### Preliminary/Postliminary Scripting Functions

The following table describes the functions you can use in a preliminary or postliminary script. The parentheses at the end of the function name contain the parameters, if any, that the function accepts.

<table>
<thead>
<tr>
<th>Function name and parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>getCallLicensesAllowed()</td>
<td><strong>Return value</strong> - The <code>&lt;integer&gt;</code> total number of calls allowed by the current license. Includes aggregate/combined counts.</td>
</tr>
<tr>
<td>getCallLicensesFree()</td>
<td><strong>Return value</strong> - The <code>&lt;integer&gt;</code> total number of calls in the license still allowed (total allowed - total used). Includes aggregate/combined counts.</td>
</tr>
<tr>
<td>getCallLicensesUsed()</td>
<td><strong>Return value</strong> - The <code>&lt;integer&gt;</code> total number of calls used from the license. Includes aggregate/combined counts.</td>
</tr>
<tr>
<td>isCallLicenseBurstEnabled()</td>
<td><strong>Return value</strong> - The <code>&lt;boolean&gt;</code> value if the Call License Burst feature is licensed and enabled (true), or if it is either not licensed or is licensed but not enabled (false).</td>
</tr>
<tr>
<td>Function name and parameters</td>
<td>Details</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| getConferenceRoomOrID()     | **Return value:**  
  ▪ For dial-outs to endpoints from VMRs or Polycom RealConnect conferences, returns the VMR or Skype Conference ID.  
  ▪ For dial-outs to the VMR or Polycom RealConnect conferences, and for dial-ins, returns the empty string. |
| getHeader(<SIP header name>) | **Return value** - The contents of the specified SIP header in the original SIP INVITE request.  
  **Note:** The return value is not changed if the SIP header is changed with setHeader. |
| setHeader(<SIP header name>, <text>) | Replaces the current contents of the specified SIP header in the output version of the SIP INVITE request with <text>.  
  **Return value:** None.  
  **Note:** Any changes made using setHeader do not affect subsequent values returned by getHeader. |
| getDisplayName(<text>)      | **Return value** - The display name portion of <text>.  
  **Note:** This function assumes that <text> uses the format of a SIP INVITE - To header. |
| getUser(<text>)              | **Return value** - The user portion of <text>.  
  **Note:** This function assumes that <text> uses the format of a SIP INVITE - To header. |
| getParameterString(<text>)   | **Return value** - Returns the parameter string portion of <text>.  
  **Note:** This function assumes that <text> uses the format of a SIP INVITE - To header. |
| appendParameterString(<header Text>, <text>) | **Return value** - Returns the result of appending <text> to the end of <headerText>, using the format of a SIP INVITE - To header. |
| removeHeader(<text>)         | Removes the header named <text> from the SIP INVITE.  
  **Return value** - None. |
| getPeerHost()                | **Return value:**  
  ▪ If invoked from an External SIP Peer postliminary script, returns the **Next hop address** configured for this SIP peer.  
  ▪ Otherwise, returns the empty string. |
### Function name and parameters

<table>
<thead>
<tr>
<th>Function name and parameters</th>
<th>Details</th>
</tr>
</thead>
</table>
| `getPeerNetOrNextHop()`     | **Return value:**  
  - If invoked from an External SIP Peer postliminary script, returns one of the following:  
    - The **Destination network** value configured for this SIP peer, if defined  
    - The **Next hop address** for this SIP peer, if the **Destination network** setting is not configured  
  - If not invoked from an External SIP Peer postliminary script, returns the empty string. |
| `getPeerPort()`              | **Return value:**  
  - If invoked from an External SIP Peer postliminary script, returns the IP network port configured for this SIP peer.  
  - Otherwise, returns the empty string. |
| `getPeerTransport()`         | **Return value:**  
  - If invoked from an External SIP Peer postliminary script, returns the **Transport type** configured for this SIP peer.  
  - Otherwise, returns the empty string. |

### How Dial Rule Actions Affect SIP Headers

The following table shows how different dial rule actions apply a preliminary script's modified dial string to the output SIP headers in a SIP call:

<table>
<thead>
<tr>
<th>Dial rule action</th>
<th>Output SIP headers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve to registered endpoint</td>
<td>The To header is replaced with the modified dial string. The request URI is based on the contact address of the registered endpoint, and not replaced with the modified dial string.</td>
</tr>
<tr>
<td>Resolve to external address</td>
<td>The To header and the request URI are both replaced with the modified dial string.</td>
</tr>
</tbody>
</table>
| Resolve to service prefix    | For a SIP peer proxy of type OCS:  
  The To header is replaced with the modified dial string. The request URI is based on the address, port, and transport type of the proxy, and not replaced with the modified dial string.  
  For a SIP peer proxy of type Other:  
  The To header and the request URI are both replaced with the modified dial string. |
<table>
<thead>
<tr>
<th>Dial rule action</th>
<th>Output SIP headers</th>
</tr>
</thead>
</table>
| Resolve to peer proxy  | For a SIP peer proxy of type **OCS**:  
The **To** header is replaced with the modified dial string. The request URI is based on the address, port, and transport type of the proxy, and not replaced with the modified dial string.  
For a SIP peer proxy of type **Other**:  
The **To** header and the request URI are both replaced with the modified dial string. |
| Resolve to IP address  | The **To** header and the request URI are both replaced with the modified dial string.                      |

## Test Preliminary and Postliminary Scripts

Script debugging enables you to test a JavaScript executable script that you’ve added as a preliminary to a dial rule or a postliminary for an external gatekeeper, SIP peer, SBC, or MCU.

You can specify parameters of a call and the dial string, and see what effect the script has on the dial string.

**Procedure**

1. Go to **Service Config > Dial Plans**.
2. Select a dial plan.
3. Select the dial rule with the script to test and click **Edit Dial Rule**.
4. On the **Preliminary** tab, select **Debug this Script**.
5. Complete the script debugging details as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Dial string          | This is the **DIAL_STRING** variable in the script, which is initially set to the dial string being evaluated. Enter a dial string to test. Alternatively, provide the entire **SIP INVITE** message. Then click **Execute Script**.  
**Note:** For SIP, the script should always specify the schema prefix (sip or sips). For example:  
**DIAL_STRING = "sip:xxx@10.33.120.58"** |
| Caller site          | Select a site in order to set the first four caller variables.                                      |
| Caller variables     | Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable. |
| VMR/transient conf ID| This field specifies the return value of the function **getConferenceRoomOrID()**.  
If the script simulates a call to a VMR or transient conference ID or a dial-in call, this field is blank. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final result</td>
<td>Displays the outcome of running the script. For a dial rule preliminary, if the script rejected the dial string (skipping the dial rule action and passing it on to the next dial rule), a message tells you so. Otherwise, the transformed dial string is displayed.</td>
</tr>
<tr>
<td>Script output</td>
<td>Displays any output produced by the script (for example, <code>println</code> statements).</td>
</tr>
<tr>
<td>Output SIP headers</td>
<td>For an external SIP peer’s postliminary, displays the headers produced by the script.</td>
</tr>
</tbody>
</table>

6. Click **Execute Script** to test the preliminary script.

## Sample Preliminary and Postliminary Scripts

A preliminary is an executable script, written in the JavaScript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule’s action is performed.

A postliminary is an executable script, written in the JavaScript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the `DIAL_STRING` variable (which is initially set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule’s action (if the filter criteria aren’t met) or return one of the following:

- **NEXT_RULE**: Skips the rule being processed and passes the dial string to the next rule.
- **BLOCK**: Rejects the call.

The following sample scripts address many of the scenarios for which you might need a preliminary or postliminary script. You can use them as templates or starting points for your scripts.

```javascript
// Example preliminary and postliminary scripts

// STRIP PREFIX
// If the dial string has prefix 99, remove it
// 991234 --> 1234
DIAL_STRING = DIAL_STRING.replace(/^99/,"");

// ADD PREFIX
// Add prefix 99 to the dial string
// 1234 --> 991234
DIAL_STRING = "99" + DIAL_STRING;

// STRIP PREFIX (SIP)
// If the dial string is a SIP URI with prefix 99 in the user part, remove it
// SIP:991234@abc.com --> sip:1234@abc.com
DIAL_STRING = DIAL_STRING.replace(/^sip:99([^@]*@)/i,"sip:$1");

// ADD PREFIX (SIP)
// If the dial string is a SIP URI, add prefix 99 to the user part
```

349
DIAL_STRING = DIAL_STRING.replace(/\^sip:\([^@]*@)/i,"sip:99$1");

// SUBSTITUTE DOMAIN (SIP)
// If the dial string is a SIP URI, change the domain part to "example.com"
// SIP:1234@abc.com  -->  sip:1234@example.com
DIAL_STRING = DIAL_STRING.replace(/\^sip:\([^@]*@(.*)/i,"sip:$1@example.com");

// FILTER
// If the dial string has prefix 99, do not match on this rule. Skip to the next rule.
// 991234  -->  NEXT_RULE
if (DIAL_STRING.match(/\^99/))
{
    return NEXT_RULE;
}

// FILTER (Inverted)
// Do not match on this rule unless the dial string has prefix 99.
// 1234  -->  NEXT_RULE
if (!DIAL_STRING.match(/\^99/))
{
    return NEXT_RULE;
}

// FILTER (SIP)
// If the dial string is a SIP URI with domain "example.com", do not match on this rule.
// Skip to the next rule.
// sip:1234@example.com  -->  NEXT_RULE
if (DIAL_STRING.toLowerCase().match(/\^sip:\[^@]*@example.com/))
{
    return NEXT_RULE;
}

// PRINTLN
// Print out the information available to the script for this call.
// Information printed using the print or println functions is saved as a call audit event, which is viewable in the DMA interface under Reports > Call History, and also in the Script Debugging dialog box.
print("DIAL_STRING: " + DIAL_STRING);
print("CALLER_SITE_NAME: " + CALLER_SITE_NAME);
print("CALLER_SITE_COUNTRY_CODE: " + CALLER_SITE_COUNTRY_CODE);
print("CALLER_SITE_AREA_CODE: " + CALLER_SITE_AREA_CODE);
print("CALLER_SITE_DIGITS: " + CALLER_SITE_DIGITS);
print("CALLER_H323ID: " + CALLER_H323ID[0]);
print("CALLER_E164: " + CALLER_E164[0]);
print("CALLER_TEL_URI: " + CALLER_TEL_URI);
print("CALLER_SIP_URI: " + CALLER_SIP_URI);

// FILTER (Site)
// Do not allow callers from the atlanta site to use this rule.
// (Caller site == "atlanta")  -->  NEXT_RULE
if (CALLER_SITE_NAME == "atlanta")
{
    return NEXT_RULE;
}
SITE BASED NUMERIC NICKNAMES
Allow caller to omit country and area code when calling locally.
Assumes that country and area codes are set in site topology.
Assumes that all endpoints are registered with their full alias, including
country and area code.
5551212 --> 14045551212
if (DIAL_STRING.length == CALLER_SITE_DIGITS)
{
  DIAL_STRING = CALLER_SITE_COUNTRY_CODE + CALLER_SITE_AREA_CODE +
  DIAL_STRING;
}
else if (DIAL_STRING.length == (parseInt(CALLER_SITE_AREA_CODE.length,10)
+ parseInt(CALLER_SITE_DIGITS,10)))
{
  DIAL_STRING = CALLER_SITE_COUNTRY_CODE + DIAL_STRING;
}
SITE BASED NUMERIC NICKNAMES (SIP)
Allow caller to omit country and area code when calling locally.
Assumes that country and area codes are set in site topology.
Assumes that all endpoints are registered with their full alias, including
country and area code.
sip:5551212@example.com --> sip:14045551212@example.com
if (DIAL_STRING.toLowerCase().match(/^sip:([^@]*@example.com)/))
{
  user = DIAL_STRING.replace(/^sip:(\^[^@]*@?\d*/i,"$1");
  if (user.length == CALLER_SITE_DIGITS)
  {
    user = CALLER_SITE_COUNTRY_CODE + CALLER_SITE_AREA_CODE + user;
  }
  else if (user.length == (parseInt(CALLER_SITE_AREA_CODE.length,10)
+ parseInt(CALLER_SITE_DIGITS,10)))
  {
    user = CALLER_SITE_COUNTRY_CODE + user;
  }
  DIAL_STRING = "sip:" + user + "@example.com";
}
LIMITING CALLS TO A CERTAIN NUMERIC DIAL RANGE.
(like the range specified Conference Settings screen)
var minGeneratedRoomId = 1000;
var maxGeneratedRoomId = 9999;
var number = parseInt(DIAL_STRING.replace(/^sip:([^@]*@[^/]*\d*/i,"$1"));
if (isNaN(number) || number > minGeneratedRoomId && number <
  maxGeneratedRoomId)
{
  return;
}
return NEXT_RULE;
A sample script that routes all dial-out calls from a
whitelist of VMRs to a SIP peer with prefix 11. All other dial-out
calls will be routed to a SIP peer with prefix 22.
The getConferenceRoomOrID() function returns a value only when
the call is a dial-out from a VMR or Skype scheduled conference
// to an endpoint.
var whitelist_vmrs = [
"1000",    // Specify list of VMRs; add or remove VMRs from this list.
"2000",    // Make sure you use the syntax "<vmr number>"<comma>
"3000",
];
var prefix = "22";

// Match against individual VMRs. ACCEPT if any of them matches.
if (0 <= whitelist_vmrs.indexOf(getConferenceRoomOrID())) {
    prefix = "11";
}
DIAL_STRING = prefix + DIAL_STRING;

// This script may be useful with "Resolve to external SIP peer" dial rules.
// This script skips this dial rule unless the call is SIP or SIPs.
// Without this, the H.323-SIP gateway function could be invoked.
if (!DIAL_STRING.match(/sips?:/i)) {
    return NEXT_RULE;
}

// This script may be useful with "Resolve to registered endpoint" dial rules.
// This script applies to registered H.323 endpoints calling registered SIP endpoints (e.g., 1001, 1002, ...) and forces a H.323-SIP gateway call by adding the "sip:" dialing scheme.
// System configuration: Replace sip.domain.com with your system's SIP domain.
DIAL_STRING = DIAL_STRING.replace(/(^1001$)/, "sip:\$1@sip.domain.com");
DIAL_STRING = DIAL_STRING.replace(/(^1002$)/, "sip:\$1@sip.domain.com");

// This script may be useful with "Resolve to registered endpoint" dial rules.
// This script applies to registered SIP endpoints calling registered H.323 endpoints (e.g., 1001, 1002, ...) and forces a SIP-H.323 gateway call by removing the dialing scheme.
// System configuration: Replace sip.domain.com with your system's SIP domain.
DIAL_STRING = DIAL_STRING.replace(/sips?:\(1001\)@sip.domain.com.*,/ "$1");
DIAL_STRING = DIAL_STRING.replace(/sips?:\(1002\)@sip.domain.com.*,/ "$1");

// This script illustrates how to accept SIP dial strings that include upper case characters and convert them into dial strings with only lower case characters. Thus, calls to sip:AbCdEfG123@MyDomain.com are converted to sip:abcdefg123@mydomain.com.
// This script can be configured as the preliminary for a dial rule with the

---

Preliminary and Postliminary Scripting
action "Resolve
// to registered endpoint".
//
// CAUTION: This script should be used in conjunction with some method to
// assure that all
// SIP registered endpoints have only lower-case characters. One way to
// assure this is to
// use this script in conjunction with a registration policy script that
// only allows
// endpoints with lower case SIP URIs to register. See "Sample Preliminary
// and
// Postliminary Scripts."
//
// Applying this script to other dial rules can cause problems with
// interoperability.
// For example, if this script is applied to calls to external SIP peers,
// then the
// endpoints that are eventually contacted through those SIP peers must
// have lower case
// SIP URIs, or the calls will fail.
//
// Convert all SIP dial strings to lower case and record instances where
// the dial string
// was changed.
//
// if (CALLER_SIP_URI != null && CALLER_SIP_URI != "") { 
var origDS = DIAL_STRING;
DIAL_STRING = DIAL_STRING.toLowerCase();
if (origDS != DIAL_STRING) {
println("Dial string case changed. Original dialstring=
" + origDS + 
"Lowered=" + DIAL_STRING);
}
}

// This script may be useful with "Resolve to registered endpoint" or
"Resolve
// to conference room ID" dial rules.
//
// This script prepends a prefix (8237) to any 4 digit dial string
beginning
// with 4, 5, or 6 (SIP or H.323).
DIAL_STRING=DIAL_STRING.replace(/^(\[4-6\][0-9]{3})$/,"8237$1");
DIAL_STRING=DIAL_STRING.replace(/^(sips?:)(\[4-6\][0-9]{3})$/,"$18237$2");
DIAL_STRING=DIAL_STRING.replace(/^(sips?:)(\[4-6\][0-9]{3})@/,"$18237$2");

// This script may be useful with "Resolve to service prefix" dial rules.
//
// This applies to PSTN or ISDN dial-outs from H.323 endpoints where the E.
164
// number is prefixed with 9.
// The MCU is configured with prefix 2082 and 001 is the gateway session
// prefix. The MCU expects ** as the delimiter for the E.164 number.
DIAL_STRING=DIAL_STRING.replace(/^9([0-9]*)$/,"2082001**$1");

// This script may be useful with "Resolve to external gatekeeper" dial
rules
// that send h323 calls to a Cisco VCS device.
//
// This script skips this dial rule if the call is SIP or SIPs. (Without
Preliminary and Postliminary Scripting

this,
// the SIP-H.323 gateway function would be invoked).
// For H.323 Annex O dial strings of the form <alias>@<domain>, this script
// prepends the dialing scheme "h323:".
if (DIAL_STRING.match(/^sips?:/i))
{
return NEXT_RULE;
}
else
{
DIAL_STRING=DIAL_STRING.replace(/^([^:@]*)@([^@]*)/,"h323:$1@$2");
println("new dial string is: " + DIAL_STRING);
}
////////////////////////////////
// This script may be useful with "Resolve to external SIP peer" dial
rules.
// System configuration: Each SIP peer selected in the dial rule is
configured
// with a prefix (11, 22, or 33).
// The script skips this dial rule for dial strings that are't SIP, whose
alias
// isn't 5 characters, or that don't specify one of the prefixes.
// For dial strings that meet these criteria, the domain is removed.
alias = DIAL_STRING.replace(/^sips?:([^@]*)@.*/i,"$1");
if (alias.length != 5)
{
return NEXT_RULE;
}
if (alias.match(/^11/) || alias.match(/^22/) || alias.match(/^33/))
{
DIAL_STRING = DIAL_STRING.replace(/(^sips?:)([^@]*)@.*/i,"$1$2");
println("new DIAL_STRING: " + DIAL_STRING);
}
else
{
return NEXT_RULE;
}
////////////////////////////////
// This script may be useful with various dial rules.
//
// This script skips this dial rule if the dial string is not a 10 digit
// number. This works for both H.323 and SIP.
alias = DIAL_STRING.replace(/^sips?:([^@]*).*/i,"$1");
if (!alias.match(/^[0-9]{10}$/))
{
return NEXT_RULE;
}
////////////////////////////////
//
This script may be useful with "Resolve to conference room ID" dial
rules.
//
//
If there are conference rooms with the same numbers as registered
endpoints,
//
this script adds a prefix for conference rooms to distinguish them.
if(CALLER_SITE_NAME.match(/USDMAs/))
{
if(!(DIAL_STRING.match(/^61*|^(sip:61|h323:61)/)))
{
if(DIAL_STRING.match(/^sip:/))

354


DIAL_STRING = DIAL_STRING.replace(/sip:([^@]*@)/i,"sip:61$1");
} else if (DIAL_STRING.match(/^h323:/))
{
DIAL_STRING = DIAL_STRING.replace(/^h323:([^@]*@)/i,"h323:61$1");
} else
{
DIAL_STRING = "61" + DIAL_STRING;
}
println("New translated DIAL_STRING: " + DIAL_STRING);
}
if(!(DIAL_STRING.match(/^61*|^(sip:61|h323:61)/))){
return NEXT_RULE;
}
Access Control

Topics:

- Access Control Lists
- Access Proxy Settings
- Media Traversal Settings
- TURN Settings
- Registration Policies
- Device Authentication

This section provides an introduction to configuring access control for the Polycom RealPresence DMA system.
Access Control Lists

Topics:

- Access Control List Rules
- Access Control List Variables
- Access Control List Settings
- Assigning ACLs to Ports

An access control list (ACL) is a list of rules that the RealPresence DMA system uses to evaluate SIP and H.323 traffic to the system's public and private signaling ports. The rules in an ACL have associated actions that define whether the RealPresence DMA system allows or denies SIP or H.323 provisioning, registration, and call requests from endpoints or other devices on a network.

The RealPresence DMA system comes with two default ACLs. You can also create custom ACLs.

Working with ACLs involves several steps:

1. Define ACL rules and their conditions.
2. Specify variables to apply to the ACL rules.
   
   **Note:** If you plan to use custom variables for a rule condition, you should define the variables first, before you create or edit the rule and its conditions.
3. Assign an action (allow or deny) to each ACL rule.
4. Add one or more rules to an ACL.
   
   You can create a custom ACL or use one of the system's default ACLs.
5. Assign an ACL to a specific SIP or H.323 port.

Access Control List Rules

The RealPresence DMA system has various default ACL rules that define access conditions for incoming traffic to the system's signaling ports.

You can use the RealPresence DMA system's default ACL rules as-is or edit them. You can also create customized ACL rules and conditions.

When you add a rule to an ACL, you need to specify whether the RealPresence DMA system will allow or deny traffic that matches the conditions of the rule.

View All Access Control List Rules

The RealPresence DMA system contains a number of pre-configured rules.

You can view a list of all system default rules and custom rules that you create.

Procedure

» Go to Service Config > Access Control > ACL Rules.
All rules display with their associated descriptions, service types, and ACLs to which they're assigned.

**Add an Access Control List Rule**

You can add custom ACL rules and specify the conditions that define each rule.

A condition includes an attribute, operator, and a value. If a rule has more than one condition, a relation defines how the conditions are applied relative to each other.

**Note:** You can define multiple conditions for each rule you create. When you define the first condition, the **Relation** field is not active. When you add subsequent conditions, select the relation for each condition.

**Procedure**

1. Go to **Service Config > Access Control > ACL Rules**.
2. Click the **Add** button.
3. Complete the following fields:
   - **Rule Name** - Enter a descriptive name for the rule. Do not use blank spaces in the name.
   - **Description** - Enter a brief summary of what the rule does.
   - **Service Type** - Select **SIP**, **H.323**, or **SIP and H.323**.
4. In the **Condition** field, click the **Add** button to add a condition for the rule and complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relation</td>
<td>You can define multiple conditions for each rule you create. When you define the first condition, the <strong>Relation</strong> field is not active. When you add subsequent conditions, you can select the relation for each condition.</td>
</tr>
<tr>
<td></td>
<td>• <strong>and</strong> - If a request meets all of the conditions in the rule, the action for the rule is applied to the request.</td>
</tr>
<tr>
<td></td>
<td>• <strong>or</strong> - If a request meets any one of the conditions in the rule, the action for the rule is applied to the request.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Attributes depend on the <strong>Service Type</strong> (<strong>SIP</strong>, <strong>H.323</strong>, or <strong>SIP and H.323</strong>) and specify the fields in the header of a SIP or H.323 request message.</td>
</tr>
<tr>
<td>Operator</td>
<td>An operator compares the <strong>Attribute</strong> and <strong>Value</strong> fields of the condition. For any attribute you choose, the operator you select determines the available values for the condition.</td>
</tr>
<tr>
<td>Value</td>
<td>The value for a condition is dependent on the attribute and operator. You can select a predefined variable (a list of values) or you can also enter a single value in this field.</td>
</tr>
</tbody>
</table>
5. Click **OK** to add the condition to the rule.
6. Select the condition, then click the **Add** button to add other conditions to the rule if needed.
7. Click **OK** to save the new rule and return to the **ACL Rules** page.
**Edit an Access Control List Rule**

You can edit ACL rules and revise the conditions (relation, attribute, operator, value) that define each rule.

**Procedure**

1. Go to **Service Config > Access Control > ACL Rules**.
2. Select the ACL rule to edit.
3. Click the **Edit** button.
4. Revise the following fields as needed:
   - **Rule Name** - Enter a descriptive name for the rule. Do not use blank spaces in the name.
   - **Description** - Enter a brief summary of what the rule does.
   - **Service Type** - Select SIP, H.323, or SIP and H.323.
5. In the **Condition** field, do one of the following:
   - If the rule doesn't have any conditions, click the **Add** button to add a new condition for the rule.
   - If the rule has conditions, select a condition, then click the **Add** button to add another condition, or click the **Edit** button to edit the condition you selected.
6. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Relation | You can define multiple conditions for each rule you create. When you define the first condition, the **Relation** field is not active. When you add subsequent conditions, you can select the relation for each condition.  
  - **and** - If a request meets all of the conditions in the rule, the action for the rule is applied to the request.  
  - **or** - If a request meets any one of the conditions in the rule, the action for the rule is applied to the request. |
| Attribute| Attributes depend on the **Service Type** (SIP, H.323, or SIP and H.323) and specify the fields in the header of a SIP or H.323 request message. |
| Operator | An operator compares the **Attribute** and **Value** fields of the condition. For any attribute you choose, the operator you select determines the available values for the condition. |
| Value    | The value for a condition is dependent on the attribute and operator. You can select a predefined variable (a list of values) or you can also enter a single value in this field. |
7. Click **OK** to save the new or revised condition.
8. Click **OK** to save the changes to the rule and return to the **ACL Rules** page.

**Copy an Access Control List Rule**

If you need to create a new ACL rule that is similar to an existing rule, you can copy the existing rule and revise it as needed.
**Procedure**

1. Go to **Service Config > Access Control > ACL Rules**.
2. Select the ACL rule to copy.
3. Click the **Copy** button.
4. Complete the following fields:
   - **Rule Name** - Enter a descriptive name for the rule. Don’t use blank spaces in the name.
   - **Description** - Enter a brief summary of what the rule does.
   - **Service Type** - Select **SIP**, **H.323**, or **SIP and H.323**.
5. Select a **Condition**, then add a new condition, or edit or delete the condition as needed.
6. Click **OK** to save the new rule and return to the **ACL Rules** page.

**Delete an Access Control List Rule**

To delete an ACL rule, you must first delete any ACL variables and rule actions for the rule, then delete the rule.

**Procedure**

1. Go to **Service Config > Access Control > ACL Rules**.
2. Select the ACL rule to delete.
3. Click the **Delete** button.
4. Click **Yes** to confirm the deletion.
   - The rule is deleted from the **ACL Rules** list.

**Access Control List Variables**

Variables can be used to define group members, source IP addresses, and other lists.

You can create custom variables and add values (list items) to the variables. A variable with its component values can then be applied to a condition for an ACL rule, depending on the attribute and operator you select for the condition.

**Note:** If you plan to create rules with one or more conditions that contain custom variables, you may want to define the variables first so they appear in the **Value** field when you add a condition that uses a custom variable.

The RealPresence DMA system maintains the following default system variables. These variables contain dynamic lists of values that the system automatically updates. They cannot be edited.

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>h323provlist</td>
<td>List of H.323 endpoints that are successfully provisioned by the RealPresence DMA Resource Manager system through the RealPresence DMA system</td>
</tr>
<tr>
<td>h323reglist</td>
<td>List of H.323 endpoints that have successfully registered to the RealPresence DMA system</td>
</tr>
<tr>
<td>Variable Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>sipprovlist</td>
<td>List of SIP endpoints that are successfully provisioned by the RealPresence DMA Resource Manager system through the RealPresence DMA system</td>
</tr>
<tr>
<td>sipreglist</td>
<td>List of SIP endpoints that have successfully registered to the RealPresence DMA system</td>
</tr>
</tbody>
</table>

The system also comes with the **SIPscanners** variable, a list of SIP scanner regular expressions (regexes). You can add values to this list when necessary.

**Add a Variable**

You can create custom variables to use in conditions for ACL rules.

**Procedure**

1. Go to **Service Config > Access Control > ACL Variables.**
2. Click the **Add** button.
3. Complete the following fields:
   - **Variable name** - Enter a name for the variable.
   - **Description** - Enter a brief description of the type of values the variable contains.
   - **Service Type** - Select **SIP**, **H.323**, or **SIP and H.323**.
   - **Value** - Click the **Add** button to enter a value to include in this variable, such as a string, number, or regular expression.
4. Click **OK** to add the value to the list of values.
5. Add more values as needed.
6. Click **OK**.

**Edit a Variable**

You can edit variables and their values when necessary.

**Procedure**

1. Go to **Service Config > Access Control > ACL Variables.**
2. Select a variable to edit and click the **Edit** button.
3. Revise the following fields as needed:
   - **Variable name** - Enter a name for the variable.
   - **Description** - Enter a brief description of the variable.
   - **Service Type** - Select **SIP**, **H.323**, or **SIP and H.323**.
   - **Value** - Select the value to revise and click the **Edit** button. You can also select a value to delete and click the **Delete** button.
4. Revise the value as needed and click **OK**.
5. Revise additional values if necessary.
6. Click **OK**.
7. Revise additional variables as needed.
Delete a Variable

Edit or delete variables when they're no longer in use.

If you try to delete a variable that a rule references, the delete action will fail.

Procedure

1. Go to Service Config > Access Control > ACL Variables.
2. Select a variable to delete and click the Delete button.
3. Click Yes to confirm the deletion.

Access Control List Settings

ACL settings are used to manage Access Control Lists, assign actions to ACL rules, and assign ACL rules to Access Control Lists.

Actions are assigned to rules and rules are assigned to ACLs.

An ACL setting combines an ACL rule with the action the RealPresence DMA system performs (allow or deny) when it evaluates the rule against incoming signaling traffic (provisioning, registration and call requests). The rule and its action must be added to an ACL, and the ACL must be assigned to a listening port. The system applies rule settings according to the order of priority you define.

The RealPresence DMA system has two default ACLs:

- **Factory Core ACL** is the default ACL applied to SIP and H.323 traffic on systems with a core configuration.
- **Factory Edge ACL** is the default ACL applied to SIP and H.323 traffic on systems with an edge configuration.

Both of the default ACLs are available on core-configured and edge-configured systems but it is recommended that you use the default ACL for your system’s configuration.

The action the RealPresence DMA system applies to the All Traffic rule in each of the default ACLs differs:

<table>
<thead>
<tr>
<th>System Configuration</th>
<th>Default Access Control List</th>
<th>All Traffic Rule Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td>Factory Core ACL</td>
<td>Allow all traffic</td>
</tr>
<tr>
<td>Edge</td>
<td>Factory Edge ACL</td>
<td>Deny all traffic</td>
</tr>
</tbody>
</table>

On a new RealPresence DMA system configured for edge, you need to change the **Provisioned Endpoints** rule action in the **Factory Edge ACL** from **Deny** to **Allow** to enable any signaling traffic to get through the system.

Add an Access Control List

The RealPresence DMA system comes with two default ACLs.

You can use these default ACLs as-is or revise them. You can also add a custom ACL that contains RealPresence DMA system default rules and/or rules that you create.
If you create a new ACL for a RealPresence DMA system in a core or an edge configuration, you can optionally create an **All Traffic** rule to include in the new ACL and configure the rule to deny all traffic. You can then create additional rules that allow traffic based on the desired outcome. When you place the **All Traffic** rule as last priority in the list of ACL rules, any traffic that doesn’t match one of the preceding rules will be denied by the **All Traffic** rule.

**Note:** An ACL must contain at least one rule. An empty ACL that's assigned to a port will deny all traffic by default.

**Procedure**

1. Go to **Service Config > Access Control > ACL Settings**.
2. Under **Access Control Lists**, click the **Add ACL** button.
3. Complete the following fields:
   - **ACL name** - Enter a name for the ACL.
   - **Description** - Enter a brief description of the ACL.
4. Click **OK** to create the new ACL.

**Edit an Access Control List**

You can revise the name and description of an existing ACL.

**Procedure**

1. Go to **Service Config > Access Control > ACL Settings**.
2. Under **Access Control Lists**, select the ACL to revise.
3. Click the **Edit ACL** button.
4. Revise the following fields as needed:
   - **ACL name** - Enter a name for the ACL.
   - **Description** - Enter a brief description of the ACL.
5. Click **OK** to save the changes.

**Copy an Access Control List**

If you need to create a new ACL that is similar to an existing ACL, you can copy the existing ACL and revise it as needed.

**Procedure**

1. Go to **Service Config > Access Control > ACL Settings**.
2. Under **Access Control Lists**, select the ACL to copy.
3. Click the **Copy ACL** button.
4. Revise the following fields as needed:
   - **ACL name** - Enter a name for the new ACL.
   - **Description** - Enter a brief description of the ACL.
5. Click **OK** to save the changes.
Delete an Access Control List

You can delete an ACL if it's no longer needed.

When you delete an ACL that contains rules, the rules will not be deleted from the RealPresence DMA system.

Procedure
1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL to delete.
3. Click the Delete ACL button.
4. Click Yes to confirm the deletion.

Export Access Control Lists

If you have more than one RealPresence DMA system, you can export all ACLs, rules, and variables from one system and import them into the other system.

When you Export ACLs, the RealPresence DMA system exports ALL ACLs, rules, and variables. You cannot selectively export an individual item by name.

Procedure
1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, click Export ACLs.
   - Depending on the web browser client you use, the system automatically saves the .json export file to your local Downloads folder, or prompts you to save the file locally.
3. If necessary, copy the export file to a USB drive to use when you import the file to a different RealPresence DMA system.

Import Access Control Lists

If you have more than one RealPresence DMA system, you can export all ACLs, rules, and variables from one system and import them to a different system.

When you Import ACLs from one RealPresence DMA system to a second system, any ACLs, rules, and variables on the second system that have the same names as those in the imported file will be overwritten during the import.

If you have two RealPresence DMA systems configured for HA, the systems share the same database so you don't need to export and import ACLs.

Procedure
1. On the RealPresence DMA system where you want to import ACLs, go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, click Import ACLs.
   - The system prompts you to confirm the import.
3. Click Yes to continue.
4. Navigate to the .json file you exported from the other RealPresence DMA system.
5. Click Open.
   - The file upload status displays.
6. Click OK to close the File Upload window.
7. Access the ACLs, rules, and variables you imported as needed.
Add an ACL Rule and Action to an ACL

You can define the action the RealPresence DMA system will take if the conditions of an ACL rule are met.

You can then add the rule and its associated action to one or more ACLs. An ACL must include at least one rule.

Procedure

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL to add an ACL rule.
3. Under Access Control Rules, click the Add Rule button.
4. Complete the following fields:
   - Rule Name - Select the rule to add to the ACL.
   - Action - Select Deny or Allow as the action the RealPresence DMA system will perform on a signaling message if the rule conditions are met.
   - Service Type - Automatically populated based on the rule.
5. Click OK to add the rule to the selected ACL.

Edit an ACL Rule Action for an ACL

You can add the same ACL Rule to different ACLs and define a different action for the rule based on the ACL it’s in.

Note: If you edit a rule action during active calls, the calls may be disrupted or terminated.

Procedure

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL with the rule whose action to edit.
3. Under Access Control Rules, select the rule to edit.
4. Click the Edit Rule button.
5. In the Action field, select Deny or Allow as the action the RealPresence DMA system will perform on a signaling message if the rule conditions are met.
6. Click OK to save the rule action.

Delete an ACL Rule from an ACL

You can delete an ACL rule from an ACL when necessary.

Note that this action removes the rule from the selected ACL but it does not delete the rule from the RealPresence DMA system.

Procedure

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL with the rule to delete.
3. Under Access Control Rules, select the rule to delete.
4. Click the Delete Rule button.
5. Click Yes to confirm the deletion.
Prioritize ACL Rules in an ACL

The RealPresence DMA system will process multiple rules within an ACL based on the priority you specify.

You can move rules up or down in an ACL to set the order in which the system processes the rules.

**Note:** A rule that allows provisioning should precede a rule that allows registration so that a device can be provisioned before it’s allowed to register.

**Procedure**

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL with the rules to prioritize.
3. Under Access Control Rules, select a rule, then click Move Rule Up or Move Rule Down to increase or decrease its priority.
4. Repeat until the rules are listed in the order you want for the selected ACL.

Disable an ACL Rule in an ACL

You can disable an ACL rule within a specific ACL without deleting the rule from the ACL.

Disabling a rule prevents the rule from being processed when the RealPresence DMA system evaluates incoming traffic on the port to which the ACL is applied.

**Procedure**

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL with the rule to disable.
3. Under Access Control Rules, select the rule to disable.
4. Click Disable ACL Rule.

   The Enabled value for the rule changes to No.

Enable an ACL Rule in an ACL

If you disable an ACL rule within a specific ACL, you can re-enable it when you want the rule to be processed again within the ACL.

**Procedure**

1. Go to Service Config > Access Control > ACL Settings.
2. Under Access Control Lists, select the ACL with the rule to enable.
3. Under Access Control Rules, select the rule to enable.
4. Click Enable ACL Rule.

   The Enabled value for the rule changes to Yes.

Assigning ACLs to Ports

An ACL needs to be assigned to each public and private listening port for SIP and H.323 signaling. The RealPresence DMA system applies the ACL to every signaling message that arrives on the port to which the ACL is assigned.

The RealPresence DMA system has two default Access Control Lists:
• **Factory Core ACL** is the default ACL applied to SIP and H.323 listening ports on systems with a core configuration.
• **Factory Edge ACL** is the default ACL applied to SIP and H.323 listening ports on systems with an edge configuration.

You can also assign a custom ACL to a SIP or H.323 port.

**Assign an ACL to a SIP Port**

You must assign an ACL for each SIP listening port.

You can specify a custom ACL or keep the default ACL that's based on the system's configuration (core or edge).

**Note:** If you edit the ACL assigned to a port during active calls, the calls may be disrupted or terminated.

**Procedure**

1. Go to **Service Config > SIP Settings**.
2. Select the port to assign the ACL to and click the **Edit** button.
3. In the **ACL** field, select the ACL to assign to the port.
4. Click **OK**.
5. Click **Update** to save the settings.

**Assign an ACL to an H.323 Port**

You must assign an ACL for each H.323 listening port.

You can specify a custom ACL or keep the default ACL that's based on the system's configuration (core or edge).

**Note:** If you edit the ACL assigned to a port during active calls, the calls may be disrupted or terminated.

**Procedure**

1. Go to **Service Config > H.323 Settings**.
2. In the **ACL** field, select the ACL to assign to the port.
3. Click **Update** to save the settings.
Access Proxy Settings

Topics:

- Add an HTTPS Proxy
- Edit an HTTPS Proxy
- Add an LDAP Proxy
- Edit an LDAP Proxy
- Add an XMPP Proxy
- Edit an XMPP Proxy
- Add a Passthrough Proxy
- Edit a Passthrough Proxy
- Add an HTTP Tunnel Proxy
- Edit an HTTP Tunnel Proxy
- Delete a Proxy
- Configure the Access Proxy Port Range

When configured as an edge server, the RealPresence DMA system provides proxy services for external devices.

You can configure access proxy settings to enable firewall and NAT traversal for sign-in and provisioning requests from remote endpoints. When the RealPresence DMA system receives a request from a remote endpoint, the system sends a new request on behalf of the remote endpoint to the appropriate application server. The RealPresence DMA system then proxies the request response from the application server to the remote endpoint. The request response directs the remote endpoint where to send registration and provisioning requests.

**Caution:** Before configuring any access proxy settings, you must configure the network interface settings for public and private access proxy IP addresses.

The RealPresence DMA system supports five types of proxies that route communication requests based on the type of target application server:

- **HTTPS Proxy** - HTTPS servers that provide management services (Polycom RealPresence Resource Manager system, Polycom ContentConnect system), and web-based video conferencing services (Polycom RealPresence Web Suite)
- **HTTP Tunnel Proxy** - RealPresence Web Suite systems that provide web-based video conferencing services.
- **LDAP Proxy** - LDAP servers that provide directory services
- **XMPP Proxy** - XMPP servers that provide message, presence, or other XMPP services
- **Passthrough Proxy** - A passthrough proxy provides transparent relay of communication requests through the RealPresence DMA system to internal application servers.

You can add proxies for different internal application servers. When you configure the proxies, you must specify an external IP address and an external listening port for access proxy. You can reuse an external
IP address but the port, in most cases, must be unique for each proxy configuration that uses the same external IP address. For example, if you create two proxy configurations for LDAP directory services, the combined external IP address for access proxy and the external listening port can’t be the same for both LDAP proxy configurations.

The following example shows some possible external IP address and port combinations.

<table>
<thead>
<tr>
<th>Name of Proxy</th>
<th>External IP Address for Access Proxy</th>
<th>External Listening Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP proxy 1</td>
<td>10.20.102.58</td>
<td>389</td>
</tr>
<tr>
<td>LDAP proxy 2</td>
<td>10.20.102.58</td>
<td>9980</td>
</tr>
<tr>
<td>HTTPS proxy</td>
<td>10.20.102.58</td>
<td>443</td>
</tr>
<tr>
<td>HTTP tunnel proxy</td>
<td>10.20.102.58</td>
<td>443</td>
</tr>
</tbody>
</table>

When adding or editing a proxy, the system validates the settings to ensure that no conflicts exist with any other proxy configurations and displays a warning message if a conflict is found.

**Add an HTTPS Proxy**

The HTTPS access proxy feature enables external users to access different internal HTTPS servers.

The RealPresence DMA system accepts a request from a remote user, then sends a new request on behalf of the user to the correct application server based on the HTTPS reverse proxy settings you configure.

When the RealPresence DMA system is integrated with a Polycom RealPresence Resource Manager system, access proxy enables remote endpoints to be provisioned and managed by the RealPresence Resource Manager system. When the RealPresence DMA system receives a login and provisioning request from an external endpoint, it sends the request to the HTTPS provisioning server configured within the RealPresence Resource Manager system.

When you configure the HTTPS Proxy settings, you can add multiple HTTPS next hops. For each next hop, you must apply a filter that's based on the HTTPS request message header received from the endpoint. The RealPresence DMA system uses the filter and other settings to send a connection request to the correct internal HTTPS application server. Two filters are available:

- **Request-URI** - The next hop is based on the Request-URI in the message header received from the endpoint. Use the Request-URI filter only when adding a next hop to a RealPresence Resource Manager system or a Polycom ContentConnect system.

- **Host header** - The next hop is based on the host information in the message header received from the endpoint. Use a host header filter when creating the next hop for various HTTPS application servers, including both the RealPresence Web Suite Services Portal and Experience Portal.

**Attention:** If you add HTTPS proxy next hops with a host header filter, you must specify the host FQDNs as subject alternative names (SANs) in the Certificate Signing Request for the RealPresence DMA system.

**Procedure**

1. Go to Service Config > Access Proxy Settings.
2. Click Add HTTPS Proxy.
3. In the **Add HTTPS Proxy Settings** window, complete the fields according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this HTTPS proxy configuration.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards HTTPS requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port at which the RealPresence DMA system listens for HTTPS proxy traffic. Default port: 443 Port range: 9950-9999 <strong>Note:</strong> The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured <strong>Access Proxy Dynamic Port Ranges</strong> on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports &lt;1024. Redirecting access proxy traffic on ports &lt;1024 to the dynamic ports enables the access proxy process to function correctly.</td>
</tr>
<tr>
<td>Require client certificate from the remote endpoint</td>
<td>When selected, the RealPresence DMA system requests and verifies the certificate of the remote endpoint. <strong>Note:</strong> Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system. Remote clients must also install a client certificate and trusted CA certificates.</td>
</tr>
<tr>
<td>Verify certificate from internal server</td>
<td>When selected, the RealPresence DMA system verifies the certificate from the internal HTTPS server (the RealPresence Resource Manager system, the Polycom ContentConnect system, or RealPresence Web Suite). <strong>Note:</strong> Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system and the RealPresence Resource Manager system.</td>
</tr>
<tr>
<td>Next hops</td>
<td>The RealPresence DMA system sends requests to the next hops you specify. For each next hop, you need to apply a filter type that's based on the HTTPS request message header received from the client. The filter types are <strong>Request-URI</strong> or <strong>Host header</strong>. The RealPresence DMA system uses the filter and other settings to send requests to the correct internal HTTPS application server.</td>
</tr>
</tbody>
</table>
4. Add the **Next Hops**.
5. Click **OK** to save the HTTPS proxy.

### Add a Next Hop

You can add a next hop that is based on the Request-URI or host information in the message header received from the endpoint.

Use the Request-URI filter only when adding a next hop to a RealPresence Resource Manager system or a Polycom ContentConnect system.

Use the Host header filter when adding a next hop to various HTTPS application servers, including the RealPresence Web Suite Experience Portal. You can also add a next hop to the RealPresence Web Suite Services Portal but should do so only if you want SIP guest clients to access the service from outside the firewall.

**Attention:** If you add HTTPS proxy next hops with a host header filter, you must specify the host FQDNs as subject alternative names (SANs) in the Certificate Signing Request for the RealPresence DMA system.

### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. Do one of the following:
   - Click **Add HTTPS Proxy** to add a new HTTPS proxy.
   - Select an existing HTTPS proxy and click **Edit**.
3. Under **Next Hops**, click **Add**.
4. Configure the settings as described in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Request-URI or Host header</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The unique name of this next hop.</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>For <strong>Request-URI</strong> next hop only. Polycom Management System, Polycom Content Sharing System (also called Polycom ContentConnect), or Other</td>
</tr>
</tbody>
</table>

**Note:** Add a separate Request-URI next hop if you need to configure HTTPS settings for both systems.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host value  | For **Host header** next hop only.  
The FQDN in the request message header that identifies the target HTTPS server being requested.  
**Note:** Use the FQDN instead of the IP address if both host header and Request-URI next hops exist simultaneously in the RealPresence DMA edge system. |
| IP address  | The private IP address of the target HTTPS server. After accepting the HTTPS request from the external endpoint, the RealPresence DMA system sends a new HTTPS request to this IP address. |
| Port        | The listening port of the internal application server. |

5. Click **OK** to save the settings.

**Edit a Next Hop**

You can edit **Request-URI** or **Host header** next hops as needed.

**Procedure**

1. Go to **Service Config > Access Proxy Settings**.
2. Select the HTTPS proxy with the next hops you want to edit and click **Edit**.
3. Under **Next Hops** in the **Edit HTTPS Proxy Settings** window, click the next hop to edit.
4. Click **Edit**.
5. Revise the settings for the **Request-URI** or **Host header** next hop as needed.
6. Click **OK** to save the settings.

**Prioritize Next Hops**

The RealPresence DMA system communicates with next hops based on the order you specify.

If you have more than one next hop for the same type of service or for different services, you can prioritize which system the RealPresence DMA DMA system contacts first when sending provisioning requests.

If your video network includes the Polycom RealPresence Web Suite, you should place the Host header next hop for RealPresence Web Suite prior to the Request-URI next hop for the RealPresence Resource Manager system to avoid potential URL overlap in the requests sent to the servers.

**Procedure**

1. Under **Next Hops** in the **Add HTTPS Proxy Settings** window, select a next hop.
2. Click **Move Priority Up** and **Move Priority Down** as needed to prioritize the next hops.
3. Click **Yes** or **No** to confirm you want to increase or decrease the priority of the next hop.
4. Click **OK** to save the priority settings.
Delete a Next Hop

You can delete any next hop that you no longer need.

Procedure
1. Go to Service Config > Access Proxy Settings.
2. Select the HTTPS proxy with the next hop you want to delete and click Edit.
3. Under Next Hops in the Edit HTTPS Proxy Settings window, click the next hop to delete.
4. Click Delete.
5. Click Yes to confirm the deletion.

Edit an HTTPS Proxy

After you add one or more HTTPS proxies, you can edit their configuration settings as needed.

Procedure
1. Go to Service Config > Access Proxy Settings.
2. From the list of proxies, select the HTTPS proxy to edit.
3. Click Edit.
4. In the Edit HTTPS Proxy Settings window, revise the following fields as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this HTTPS proxy configuration.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards HTTPS requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for HTTPS proxy traffic. Default HTTPS port: 443 Port range: 9950-9999</td>
</tr>
</tbody>
</table>

**Note:** The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured Access Proxy Dynamic Port Ranges on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports <1024. Redirecting access proxy traffic on ports <1024 to the dynamic ports enables the access proxy process to function correctly.
Add an LDAP Proxy

LDAP proxies can access different LDAP directory servers, such as the RealPresence Resource Manager LDAP server or an Active Directory server.

If you configure more than one LDAP proxy with the same public IP address, you must assign a port other than 389 to one of the proxies.

Procedure

1. Go to Service Config > Access Proxy Settings.
2. Click Add LDAP Proxy.
3. In the Add LDAP Proxy Settings window, complete the fields according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this LDAP proxy configuration</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards LDAP requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for LDAP traffic. Default LDAP port: 389 Port range: 9950-9999 Note: The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured Access Proxy Dynamic Port Ranges on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports &lt;1024. Redirecting access proxy traffic on ports &lt;1024 to the dynamic ports enables the access proxy process to function correctly.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The private IP address of the target LDAP server. The RealPresence DMA system sends a new request to the next hop IP address on behalf of the remote client.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port on which the internal LDAP server listens. Default LDAP port: 389</td>
</tr>
<tr>
<td>Require client certificate from the remote endpoint</td>
<td>When selected, the RealPresence DMA system requests and verifies the certificate of the remote endpoint. Note: Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system. Remote clients must also install a client certificate and trusted CA certificates.</td>
</tr>
<tr>
<td>Verify certificate from internal server</td>
<td>When selected, the RealPresence DMA system verifies the certificate from the internal LDAP server. Note: Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system and the RealPresence Resource Manager system.</td>
</tr>
</tbody>
</table>

4. Click OK to save the settings.

**Edit an LDAP Proxy**

You can change the settings for an LDAP proxy when necessary.

**Procedure**

1. Go to Service Config > Access Proxy Settings.
2. From the list of proxies, select the LDAP proxy to edit.
3. Click **Edit**.
4. In the **Edit LDAP Proxy Settings** window, revise the following fields as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this LDAP proxy configuration.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards LDAP requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for LDAP traffic. Default LDAP port: 389 Port range: 9950-9999. Note: The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured <strong>Access Proxy Dynamic Port Ranges</strong> on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports &lt;1024. Redirecting access proxy traffic on ports &lt;1024 to the dynamic ports enables the access proxy process to function correctly.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The private IP address of the target LDAP server. The RealPresence DMA system sends a new request to the next hop IP address on behalf of the remote client.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port on which the internal LDAP server listens. Default LDAP port: 389.</td>
</tr>
<tr>
<td>Require client certificate from the remote endpoint</td>
<td>When selected, the RealPresence DMA system requests and verifies the certificate of the remote endpoint. Note: Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system. Remote clients must also install a client certificate and trusted CA certificates.</td>
</tr>
<tr>
<td>Verify certificate from internal server</td>
<td>When selected, the RealPresence DMA system verifies the certificate from the internal LDAP server. Note: Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system and the RealPresence Resource Manager system.</td>
</tr>
</tbody>
</table>
5. Click **OK** to save the settings.

## Add an XMPP Proxy

XMPP proxies can access different XMPP servers, such as the RealPresence Resource Manager XMPP server or a different network server that provides message, presence, or other XMPP services.

### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. Click **Add XMPP Proxy**.
3. In the **Add XMPP Proxy Settings** window, complete the fields according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this XMPP proxy configuration</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards XMPP requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for XMPP traffic.</td>
</tr>
<tr>
<td></td>
<td>Default XMPP port: 5222</td>
</tr>
<tr>
<td></td>
<td>Port range: 9950-9999</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The private IP address of the target XMPP server. The RealPresence DMA system sends a new request to the next hop IP address on behalf of the remote client.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port on which the internal XMPP application server listens.</td>
</tr>
<tr>
<td></td>
<td>Default XMPP port: 5222</td>
</tr>
<tr>
<td>Require client certificate from the remote endpoint</td>
<td>When selected, the RealPresence DMA system requests and verifies the certificate of the remote endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system. Remote clients must also install a client certificate and trusted CA certificates.</td>
</tr>
</tbody>
</table>
Verify certificate from internal server

When selected, the RealPresence DMA system verifies the certificate from the internal XMPP server.

**Note:** Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence DMA system and the RealPresence Resource Manager system.

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

## Edit an XMPP Proxy

You can change the settings for an XMPP proxy when necessary.

### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. From the list of proxies, select the XMPP proxy to edit.
3. Click **Edit**.
4. In the **Edit XMPP Proxy Settings** window, revise the following fields as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this XMPP proxy configuration</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards XMPP requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for XMPP traffic. Default XMPP port: 5222 Port range: 9950-9999</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The private IP address of the target XMPP server. The RealPresence DMA system sends a new request to the next hop IP address on behalf of the remote client.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port on which the internal XMPP application server listens. Default XMPP port: 5222</td>
</tr>
</tbody>
</table>
### Add a Passthrough Proxy

A passthrough proxy provides transparent relay of communication requests through the RealPresence DMA system to internal application servers.

**Caution:** For security purposes, use of a passthrough proxy is not recommended. However, if you choose to use this function, follow the configuration instructions.

#### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. Click **Add Passthrough Proxy**.
3. In the **Add Passthrough Proxy Settings** window, complete the fields according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this passthrough proxy.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
<tr>
<td>Private IP address</td>
<td>The private access proxy IP address of the RealPresence DMA system (specified when you configure network settings). The system forwards passthrough requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Public listening port</td>
<td>The public port on which the RealPresence DMA system listens for passthrough traffic. Default passthrough ports: 8080, 80, 443 Port range: 9950-9999</td>
</tr>
</tbody>
</table>
Edit a Passthrough Proxy

You can revise a passthrough proxy as needed if the settings change.

Procedure
1. Go to Service Config > Access Proxy Settings.
2. From the list of proxies, select the passthrough proxy to edit.
3. Click Edit.
4. In the Edit Passthrough Proxy Settings window, revise the following fields as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next hop address</td>
<td>The internal IP address of the target application server. The RealPresence DMA system sends a new request to the next hop IP address on behalf of the remote client.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port on which the internal application server listens. Can be virtually any port that app server is running on.</td>
</tr>
</tbody>
</table>

5. Click OK to save the settings.
Add an HTTP Tunnel Proxy

An HTTP tunnel proxy enables SIP guest users to attend web-based video conferences hosted by the Polycom RealPresence Web Suite.

Some restrictive networks block outgoing UDP-based traffic and can limit outgoing TCP traffic to ports 80 and 443. In these situations, if a SIP guest client cannot establish a native SIP/RTP connection to a RealPresence Web Suite video conference, the RealPresence DMA system can act as a web proxy to tunnel the SIP guest call on port 80, 443, or on a port in the 9950-9999 range. Once the SIP client is connected to a meeting, the RealPresence DMA system continues to tunnel TCP traffic, including SIP signaling, media, and binary floor control protocol (BFCP) content.

The RealPresence Web Suite client uses auto-discovery to ensure that a SIP guest call is routed through the HTTP tunnel proxy when necessary. When a RealPresence Web Suite SIP guest user attempts to join a meeting, auto-discovery determines if standard SIP and media ports are reachable for the call. If not, the call is routed through the HTTP tunnel proxy.

An HTTP tunnel proxy and an HTTPS proxy can both use port 443 on the same external access proxy IP address. If you configure a port other than 443 as the external listening port for HTTP tunnel proxy calls, these calls may fail if the SIP guest client's network blocks outgoing traffic to other ports.

The following conditions apply to the HTTP tunnel proxy:
- Only one HTTP tunnel proxy can be configured.
- The HTTP tunnel proxy does not support SVC video conferencing.
- Use of an HTTP tunnel proxy is not supported with two RealPresence DMA systems deployed in a VPN tunnel configuration.

Before you configure an HTTP tunnel proxy, complete the following steps:
- Assign public access proxy IP addresses in network settings.
- Add an HTTPS proxy and configure the RealPresence Web Suite Experience Portal as a next hop.

Procedure

1. Go to Service Config > Access Proxy Settings.
2. Click Add HTTP Tunnel Proxy.
3. In the Add HTTP Tunnel Proxy Settings window, complete the fields according to the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this HTTP Tunnel proxy.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public listening port</td>
<td>The public port at which the RealPresence DMA system listens for HTTPS proxy traffic. Default HTTP port: 443 or 80. Port range: 9950-9999. <strong>Note:</strong> The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured Access Proxy Dynamic Port Ranges on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports &lt;1024. Redirecting access proxy traffic on ports &lt;1024 to the dynamic ports enables the access proxy process to function correctly.</td>
</tr>
</tbody>
</table>

4. Click **OK** to save the HTTP tunnel proxy.

## Edit an HTTP Tunnel Proxy

You can change the name and public listening port of an HTTP tunnel proxy if necessary.

To change the **Public IP address**, you need to revise the public interface setting for access proxy services in **Network Settings**.

### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. From the list of proxies, select the HTTP tunnel proxy to edit.
3. Click **Edit**.
4. In the **Edit HTTP Tunnel Proxy Settings** window, revise the following fields as needed:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this HTTP Tunnel proxy.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public IP address of the RealPresence DMA system network interface that receives access proxy traffic (specified when you configure network settings).</td>
</tr>
</tbody>
</table>
## Public Listening Port

The public port at which the RealPresence DMA system listens for HTTPS proxy traffic.

- Default HTTP port: 443 or 80
- Port range: 9950-9999

Note: The RealPresence DMA system automatically redirects inbound access proxy traffic on ports 443 and 389 to ports from the configured **Access Proxy Dynamic Port Ranges** on the access proxy public interface. The CentOS operating system does not allow processes without root ownership to listen on ports `<1024`. Redirecting access proxy traffic on ports `<1024` to the dynamic ports enables the access proxy process to function correctly.

5. Click **OK** to save the settings.

## Delete a Proxy

You can delete a proxy configuration if it is not in use.

Deleting a proxy while it is in use will terminate related active sessions and conferences.

### Procedure

1. Go to **Service Config > Access Proxy Settings**.
2. From the list of proxies, select the proxy to delete.
3. Click **Delete**.
4. Click **OK** to confirm the deletion.

## Configure the Access Proxy Port Range

You can configure the range of dynamic source ports for access proxy services.

Access proxy dynamic ports are not related to the number of calls on a license and the full range of ports is available by default. You can specify both the first and last port numbers to limit the range for access proxy, however, changing the first port number in the range is not recommended.

Each dynamic mode client uses three ports (HTTPS provisioning, LDAP, and XMPP presence). Each RealPresence Web Suite client and Polycom ContentConnect client use one port.

Dynamic port ranges configured for the RealPresence DMA system must be configured correspondingly on your firewall.

Caution: The specific ports and port ranges you configure in the RealPresence DMA system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

The following table summarizes dynamic source port information for the access proxy feature.
## Access Proxy Settings

<table>
<thead>
<tr>
<th>Service</th>
<th>First Port</th>
<th>Last Port</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access proxy dynamic source ports</td>
<td>10000</td>
<td>13000</td>
<td>The network interfaces with access proxy services assigned.</td>
</tr>
</tbody>
</table>

If you change the port range settings, the RealPresence DMA system validates the new settings to ensure that no overlap occurs among any of the port range settings for the various RealPresence DMA system services. Additionally, the system checks the port ranges to confirm the following:

- No first port number is less than 1024.
- No last port number is greater than 65535.

### Procedure

1. Go to Service Config > Access Proxy Settings.
2. Do one of the following:
   - Click Port Range Settings.
   - Click Show More, then click Port Range Settings.
3. For Access proxy dynamic ports, enter the First Port and Last Port numbers of the port range.
4. Click OK.
5. Click Yes to confirm the settings.

### Restore the Default Access Proxy Port Range

The default access proxy port range is 10000-13000.

If you change the port range, you can restore the default settings if necessary.

### Procedure

1. Go to Service Config > Access Proxy Settings.
2. Do one of the following:
   - Click Port Range Settings.
   - Click Show More, then click Port Range Settings.
3. Click Restore Defaults, then click OK.
4. Click Yes to confirm the settings.
Media Traversal Settings

Topics:

- Configure Media Traversal Settings
- Configure the Media Traversal Port Range

The media traversal feature of the RealPresence DMA system enables audio, video, and content traffic to traverse the firewall during SIP and H.323 calls.

Media traversal can be enabled on a RealPresence DMA edge-configured system that communicates with a core-configured system, another edge-configured system, or a combination system.

Configure Media Traversal Settings

You can enable media traversal for all incoming and outgoing calls.

You can also configure media relay for individual dial rules in a dial plan. The RealPresence DMA system will relay a call's negotiated media if the system resolves the call with a dial rule that's configured to have media relayed.

If a SIP or H.323 call has a negotiated media channel that is idle (no traffic is being sent or received), you can specify the number of seconds (Idle Port Timeout) after which the RealPresence DMA system will free the resources being used for the call's media setup. The resources can then be used for other calls. This option prevents the system's network resources from being held by calls that are not using them. Freeing resources does not impact active calls or signaling; any network traffic over a relayed port prevents the port from being marked idle. When a call ends normally, all associated resources are immediately released.

Procedure

1. Go to Service Config > Media Traversal Settings.
2. Select Enable media traversal.
3. Complete the fields as described in the following table.

   Note that not all fields are editable from the Media Traversal Settings page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to all calls</td>
<td>When selected, this option overrides the Relay Media setting of all dial rules in all dial plans. The RealPresence DMA system will relay media for every SIP, H.323, or SIP/H.323 gateway call that it routes.</td>
</tr>
<tr>
<td>Public media-traversal IPv4 address</td>
<td>The IP address of the network interface on the public side that has media traversal services assigned.</td>
</tr>
<tr>
<td>Private media-traversal IPv4 address</td>
<td>The IP address of the network interface on the private side that has media traversal services assigned.</td>
</tr>
<tr>
<td>Internal port range</td>
<td>The dynamic port range for private media traversal ports.</td>
</tr>
<tr>
<td>External port range</td>
<td>The dynamic port range for public media traversal ports.</td>
</tr>
</tbody>
</table>
Configure the Media Traversal Port Range

You can configure the range of dynamic source ports for media traversal services. The total ports required for each call may vary based on the signaling negotiations used to set up the call. The default media traversal port range provides the best balance between maximum calls the RealPresence DMA system can support, and the required number of open firewall ports. Reducing the range may limit the maximum number of calls for which the system can provide relay services; apply caution if changing the range is necessary.

Caution: The specific ports and port ranges you configure in the RealPresence DMA system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

The following table summarizes dynamic source port information for media traversal services.

<table>
<thead>
<tr>
<th>Service</th>
<th>First Port</th>
<th>Last Port</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media traversal dynamic source ports (private)</td>
<td>40002</td>
<td>45500</td>
<td>The network interfaces on the private side with media traversal services assigned.</td>
</tr>
<tr>
<td>Media traversal dynamic source ports (public)</td>
<td>23002</td>
<td>28500</td>
<td>The network interfaces on the public side with media traversal services assigned.</td>
</tr>
</tbody>
</table>

If you change the port range settings, the RealPresence DMA system validates the new settings to ensure that no overlap occurs among any of the port range settings for RealPresence DMA system services. Additionally, the system checks the port ranges to confirm the following:

- No first port number is less than 1024.
- No last port number is greater than 65535.

Procedure

1. Go to Service Config > Media Traversal Settings.
2. Click Port Range Settings.
3. For Media traversal dynamic ports (private), enter the First Port and Last Port numbers of the port range.
4. For Media traversal dynamic ports (public), enter the First Port and Last Port numbers of the port range.
5. Click OK.
6. Click Yes to confirm the settings.

**Restore the Default Media Traversal Port Range**
If you change the default media traversal port ranges, you can restore the defaults if necessary.

**Procedure**
1. Go to Service Config > Media Traversal Settings.
2. Click Port Range Settings.
3. Click Restore Defaults, then click OK.
4. Click Yes to confirm the settings.
TURN Settings

Topics:
- How Allocations Work
- Configure TURN Settings
- TURN Users
- Configure the TURN Port Range
- View TURN Allocations

Web Real-Time Communication (WebRTC) provides high-quality video and audio communication capabilities in some web browsers, without requiring installation of a custom plug-in.

By using Google Chrome, users both inside and outside your enterprise network can attend web-based Polycom RealPresence Web Suite conferences. In these conferences, media is exchanged directly between WebRTC clients (mesh conference) or between WebRTC clients and a Polycom MCU.

To support WebRTC-based video conferencing, the RealPresence DMA system implements both session traversal utilities for NAT (STUN) and traversal using relays around NAT (TURN) protocols. When needed, a RealPresence DMA edge-configured or combination-configured system can act as a STUN and TURN server to enable firewall and network address translation (NAT) traversal of UDP media traffic between WebRTC clients.

TURN is necessary when a WebRTC client wants to communicate with a peer but can't do so because both client and peer are behind respective NATs. STUN isn't an option if one of the NATs is a symmetric NAT (known to be non-STUN compatible). TURN is also needed when direct UDP media cannot be exchanged for other reasons (for example, due to an organization's firewall policies). Using the TURN protocol, a WebRTC client can allocate a media relay port on the TURN server that the far end can use to indirectly send media to the WebRTC client.

When you enable and configure the TURN server and a TURN user, internal and external WebRTC clients can request TURN media relay services.

How Allocations Work

All TURN messages are associated with an allocation.

To initiate a RealPresence Web Suite WebRTC conference, a WebRTC client sends an allocation request to the TURN server. Once the TURN server authenticates the request, it creates an allocation and sends a response to the client. The response contains a relayed transport address that specifies the IP address and port on the TURN server that the WebRTC client and peer can use to have the TURN server relay media between them. The relayed transport address uniquely identifies an allocation.

Typically, one allocation is created between the WebRTC client that initiates the allocation request and each peer with which it communicates. In a call with fewer than four endpoints (a WebRTC mesh call), an allocation is required for each peer-to-peer connection. For example, if three users attend a conference, each peer typically has two allocations, one for each other peer on the call.

The RealPresence DMA system supports up to 1200 allocations.
Configure TURN Settings

It's recommended that you configure a single network interface for TURN services.

When a RealPresence DMA edge-configured or combination-configured system is deployed behind a NAT, the relayed transport address sent in the allocation response to external endpoints and MCUs should always be the public IP address mapped on your firewall that corresponds to the public IP address of the network interface you assigned to TURN services. Internal endpoints and MCUs should point to the internal IP address of the network interface.

**Note:** If you deploy two RealPresence DMA systems for HA, the TURN settings (including TURN users) that you configure in one system will propagate to the other system.

**Caution:** When you enable the TURN server for the first time, you must add at least one TURN user so the TURN server will allow requests. If you disable the TURN server, all TURN users are saved and will be available if you later re-enable the TURN server.

**Procedure**

1. If you haven't already done so, go to Admin > Server > Network Settings > Services and assign a Private (LAN) and Public (WAN) interface to TURN Services. It's recommended that you assign TURN services to only a single NIC.
2. Go to Service Config > TURN Settings.
3. Select Enable TURN server.
4. Complete the fields as described in the following table.

   Note that not all fields are editable from the TURN Settings page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listening IPs</td>
<td></td>
</tr>
<tr>
<td>Public IP address</td>
<td>The public (WAN) IP address of the network interface assigned to TURN services. Automatically populated with the value from Network Settings.</td>
</tr>
<tr>
<td>Public NAT address</td>
<td>The NAT address of the network interface assigned to TURN services, mapped on the external firewall. The value displays only if you entered an IPv4 NAT address for the network interface assigned to TURN Services in Network Interface Settings.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol used for communication between the WebRTC client and the TURN server. Default: UDP</td>
</tr>
<tr>
<td>TURN port</td>
<td>The listening port the RealPresence DMA system uses to receive TURN allocation requests from private or public clients. The system uses this port only to establish a TURN session. Default UDP port: 3478</td>
</tr>
</tbody>
</table>
## TURN Users

The TURN server requires authentication of all relay allocation requests.

When the TURN server receives an unauthorized initial allocation request from a WebRTC or MCU client, the TURN server responds with its realm and the TURN user credentials a WebRTC client or MCU (TURN user) must use to authenticate further requests with the TURN server. The credentials include the username and password to be used with the realm of the TURN server.

### Add a TURN User

You need to configure one TURN user to enable WebRTC clients to request TURN services for RealPresence Web Suite mesh or bridge conferences.

Once you configure the TURN user, you must share the credentials with the system administrator for the RealPresence Web Suite system, who will complete further configurations for that product.

**Procedure**

1. Go to **Service Config** > **TURN Settings**.
2. Under **TURN Users**, click the **Add** button.
3. Complete the following required fields:
   - **Username** - The username that a WebRTC client uses to authenticate requests to the TURN server. Maximum of 20 characters.
   - **Realm** - The domain name of the RealPresence DMA TURN server. When you configure one user for the RealPresence Web Suite WebRTC clients and MCUs, the **Realm** should be the same as the **Default Authentication Realm** you configured in TURN Settings. Maximum of 20 characters.
   - **Password** - The password that a WebRTC client uses in combination with the username to authenticate its TURN requests. Maximum of 20 characters.
   - **Confirm Password** - Re-enter the password to confirm.
4. Click **OK** to add the TURN user.
5. Click **Update** to save the **TURN Users** settings.
**Edit a TURN User**

You can edit the username, realm, and password for a TURN user when necessary.

**Procedure**
1. Go to **Service Config > TURN Settings**.
2. Under **TURN Users**, select the user to edit.
3. Click the **Edit** button.
4. Revise the following required as needed:
   - **Username** - The username that a WebRTC client uses to authenticate requests to the TURN server. Maximum of 20 characters.
   - **Password** - The password that a WebRTC client uses in combination with the username to authenticate its TURN requests. Maximum of 20 characters.
   - **Confirm Password** - Re-enter the password to confirm.
5. Click **OK** to save the changes.
6. Click **Update** to save the revised **TURN Users** information.

**Configure the TURN Port Range**

You can configure the range of dynamic source ports for TURN relay services.

The number of dynamic ports you specify doesn't always map to the number of calls that can be supported. The number of ports required to support all WebRTC calls varies if the conference uses mesh mode versus bridge mode. It's recommended that you use the default relay port range listed in the TURN settings since the number of allocations can vary for calls, but you can choose any port range within the allowable range. The port range you configure must be mapped on your firewall.

**Caution:** The specific ports and port ranges you configure in the RealPresence DMA system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

The following table summarizes dynamic source port information for TURN services.

<table>
<thead>
<tr>
<th>Service</th>
<th>First Port</th>
<th>Last Port</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>TURN relay dynamic source ports</td>
<td>60002</td>
<td>65535</td>
<td>The network interfaces that have TURN services assigned.</td>
</tr>
</tbody>
</table>

If you change the port range settings, the RealPresence DMA system validates the new settings to ensure that no overlap occurs among any of the port range settings for the various RealPresence DMA system services. Additionally, the system checks the port ranges to confirm the following:

- No first port number is less than 1024.
- No last port number is greater than 65535.

**Procedure**
1. Go to **Service Config > TURN Settings**.
2. Click Port Range Settings.
3. For TURN, enter the listening port the RealPresence DMA system uses to receive TURN allocation requests from private or public clients (default port is 3478).
4. For TURN relay, enter the First Port and Last Port numbers for the port range.
5. Click OK.
6. Click Yes to confirm the settings.
7. Click Update to save the port range settings.

**Restore the Default TURN Relay Port Range**

If you change the default TURN relay port range, you can restore the default settings if necessary.

The default TURN relay port range is 60002 - 65535.

**Procedure**

1. Go to Service Config > Media Traversal Settings.
2. Click Port Range Settings.
3. Click Restore Defaults, then click OK.
4. Click Yes to confirm the settings.

**View TURN Allocations**

After the TURN server creates allocations, you can view details about them.

The number of allocations on the TURN server may not correspond with the number of calls in progress. Typically, each WebRTC client will create one TURN allocation for each peer with which it needs to connect. The ICE candidate selection process then determines the most efficient path available, so individual allocations may not be needed if the media can be sent directly to a host or server-reflexive address or through an existing TURN relay allocated by a peer client. Unused allocations will expire 10 minutes after media relay transfer begins. Typically, one allocation will remain active per leg for the duration of the call.

**Procedure**

1. Go to Monitoring > TURN Allocations.
2. Review details about the allocations, as described in the following table:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>An identifier created by the TURN server when a TURN allocation is created.</td>
</tr>
<tr>
<td>User</td>
<td>The TURN user (WebRTC client or MCU).</td>
</tr>
<tr>
<td>Realm</td>
<td>The domain name of the TURN server.</td>
</tr>
<tr>
<td>Client IP address</td>
<td>IP address of the WebRTC client that requested the allocation.</td>
</tr>
<tr>
<td>Relay IP address</td>
<td>IP address on the TURN server that the WebRTC client and peer use to have the TURN server relay media between them. Uniquely identifies the allocation.</td>
</tr>
<tr>
<td>Server IP address</td>
<td>IP address of the RealPresence DMA TURN server.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Age (sec)</td>
<td>The number of seconds since the TURN server created the allocation.</td>
</tr>
<tr>
<td>Expires (sec)</td>
<td>The number of seconds after which the allocation will expire.</td>
</tr>
</tbody>
</table>
Registration Policies

Topics:

- View Registration Policies
- Registration Policy Scripting
- Add a Registration Policy
- Edit a Registration Policy
- Copy a Registration Policy
- Delete a Registration Policy
- Assigning Registration Policies to Ports
- Sample Registration Policy Scripts

In the RealPresence DMA system, you can configure multiple policies to control registration by endpoints. The system comes with two default registration policies. These can be used as-is or you can edit them. You can also define custom registration policies.

A registration policy must be assigned to all listening SIP and H.323 ports. When you initially install your system, the default registration policy that's applied to ports is based on your system configuration, core or edge. You can keep your system's default registration policy or you can create custom policies to fit your needs.

Each registration policy contains the following components:

- **Compliance policy** - Includes an executable script (using the JavaScript language) that specifies the criteria for determining whether an endpoint is compliant or non-compliant with the registration policy.

- **Admission policy** - Specifies the action the system takes when an endpoint is compliant or non-compliant. You can choose from the following actions:
  - **Accept registration** - The endpoint's registration request is accepted and its status becomes **Active**.
  - **Block registration** - The endpoint's registration request is rejected and its status becomes **Blocked**. The system automatically rejects registration attempts (and unregistration attempts) from blocked endpoints without applying the registration policy. The status remains unchanged until you manually unblock the endpoints.
  - **Quarantine registration** - The endpoint's registration request is accepted, but its status becomes **Quarantined**. It cannot make or receive calls. The system processes registration attempts (and unregistration attempts) from quarantined endpoints, but doesn't apply the registration policy. An endpoint's status remains either **Quarantined** if registered or **Quarantined (Inactive)** if unregistered until you manually remove it from quarantine.
  - **Reject registration** - The endpoint's registration request is rejected and its status remains not registered. It doesn't appear in the **Endpoints** list. Whether it can make and receive calls depends on the system's rogue call policy. If the endpoint sends another registration request, the system applies the registration policy to that request.

Related Links
Add an Endpoint on page 524
View Registration Policies

The RealPresence DMA system's Registration Policies page includes a list of registration policies and details about each policy.

The RealPresence DMA system has two default registration policies. The Factory Core Registration Policy default compliant action is ALLOW. The Factory Edge Registration Policy default compliant action is based on provisioning. Endpoints must be provisioned to be compliant with the registration policy and be allowed to register.

Procedure

» Go to Service Config > Access Control > Registration Policies.

The following details display for each registration policy:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the registration policy.</td>
</tr>
<tr>
<td>Siteless Registration</td>
<td><strong>True</strong> - The registration policy allows registrations from endpoints that do not belong to a site.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> - The registration policy does not allow registrations from endpoints that do not belong to a site.</td>
</tr>
<tr>
<td>Devices</td>
<td><strong>True</strong> - The registration policy applies to new registrations or registrations from changed endpoints.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> - The registration policy applies only to new registrations.</td>
</tr>
<tr>
<td>IP/Port Changes</td>
<td><strong>True</strong> - The system won't reapply the registration policy if an endpoint only has IP address or port changes.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> - The system will reapply the registration policy even if an endpoint only has IP address or port changes.</td>
</tr>
<tr>
<td>Compliant Action</td>
<td>The action the system takes when an endpoint is compliant with the registration policy. Actions include:</td>
</tr>
<tr>
<td></td>
<td>• Accept registration</td>
</tr>
<tr>
<td></td>
<td>• Block registration</td>
</tr>
<tr>
<td></td>
<td>• Quarantine registration</td>
</tr>
<tr>
<td></td>
<td>• Reject registration</td>
</tr>
<tr>
<td>Noncompliant Action</td>
<td>The action the system takes when an endpoint is non-compliant with the registration policy.</td>
</tr>
<tr>
<td></td>
<td>• Accept registration</td>
</tr>
<tr>
<td></td>
<td>• Block registration</td>
</tr>
<tr>
<td></td>
<td>• Quarantine registration</td>
</tr>
<tr>
<td></td>
<td>• Reject registration</td>
</tr>
<tr>
<td>Signaling Port Assignments</td>
<td>The ports to which the registration policy is assigned.</td>
</tr>
</tbody>
</table>
Registration Policy Scripting

A registration policy script is an executable script, written in the JavaScript language, that defines the criteria the RealPresence DMA system applies to registration requests to assess whether the requests are compliant or non-compliant.

The script can specify various criteria and can be as broad or narrow as you want.

A script can return **COMPLIANT** or **NONCOMPLIANT**. A script can also assign a value (up to 1000 characters) to the EP_EXCEPTION variable. This variable’s initial value is blank (empty string). Assigning a non-blank value to the variable causes an exception to be recorded for an endpoint that requests registration. Exceptions appear on the **Endpoints** page, and you can search for endpoints with exceptions.

**Related Links**

- [Sample Registration Policy Scripts](#) on page 402

Registration Policy Script Predefined Variables

The RealPresence DMA system includes predefined variables you can use in a registration policy script.

Each time the script runs, it gets the initial values for these variables from the registration request being processed. The script can evaluate a variable or change its value (the change isn’t preserved after the script completes).

The following table describes the predefined variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Initial value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP_DEFINED_IN_CMA</td>
<td><strong>TRUE</strong> if the RealPresence DMA system is integrated with a RealPresence Resource Manager system and the endpoint is defined in that system.</td>
</tr>
<tr>
<td>EP_H323_DIALEDDIGITS_ALIAS</td>
<td>Endpoint alias value associated with H.323 dialedDigits or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_EMAIL_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 email-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_H323_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 H323-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_H323_TRANSPORT_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 transportID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>Variable</td>
<td>Initial value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EP_H323_URL_ID_ALIAS</td>
<td>Endpoint alias value associated with H.323 URL-ID or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_IP</td>
<td>Endpoint IP address. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.</td>
</tr>
<tr>
<td>EP_IS_IPV4</td>
<td><strong>TRUE</strong> if EP_IP is an IPv4 address. Blank otherwise.</td>
</tr>
<tr>
<td>EP_IS_IPV6</td>
<td><strong>TRUE</strong> if EP_IP is an IPv6 address. Blank otherwise.</td>
</tr>
<tr>
<td>EP_MODEL</td>
<td>Endpoint model.</td>
</tr>
<tr>
<td>EP_OWNER</td>
<td>Endpoint owner.</td>
</tr>
<tr>
<td>EP_OWNER_DOMAIN</td>
<td>Endpoint owner's domain.</td>
</tr>
<tr>
<td>EP_REG_IS_H323</td>
<td><strong>TRUE</strong> if the registration request uses H.323 signaling. Blank otherwise.</td>
</tr>
<tr>
<td>EP_REG_IS_SIP</td>
<td><strong>TRUE</strong> if the registration request uses SIP signaling. Blank otherwise.</td>
</tr>
<tr>
<td>EP_SIP_SIP_URI_ALIAS</td>
<td>Endpoint alias value associated with SIP sip: URI or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_SIP_SIPS_URI_ALIAS</td>
<td>Endpoint alias value associated with SIP SIPS: URI or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_SIP_TEL_URI_ALIAS</td>
<td>Endpoint alias value associated with SIP TEL: URI or blank. This is an array that can contain multiple values. Separate the values with commas.</td>
</tr>
<tr>
<td>EP_VERSION</td>
<td>Endpoint software version number.</td>
</tr>
<tr>
<td>REG_IS_PERMANENT</td>
<td><strong>TRUE</strong> if endpoint is already permanently registered. Blank otherwise.</td>
</tr>
<tr>
<td>REG_SITE_AREA_CODE</td>
<td>Area code of the site where the endpoint is attempting to register.</td>
</tr>
<tr>
<td>REG_SITE_COUNTRY_CODE</td>
<td>Country code of the site where the endpoint is attempting to register.</td>
</tr>
</tbody>
</table>
### Variable Initial value

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SITE_DIGITS</td>
<td>Number of digits in the subscriber number configured for the site where the endpoint is attempting to register.</td>
</tr>
<tr>
<td>REG_SITE_NAME</td>
<td>Site where endpoint is attempting to register.</td>
</tr>
<tr>
<td>REG_SUBNET_IP_ADDRESS</td>
<td>IP address of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.</td>
</tr>
<tr>
<td>REG_SUBNET_MASK</td>
<td>IP mask of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.</td>
</tr>
<tr>
<td>Is endpoint provisioned</td>
<td>When checked, the script simulates an endpoint provisioned by a RealPresence Resource Manager system or a Polycom ContentConnect system.</td>
</tr>
<tr>
<td>Is endpoint registered</td>
<td>When checked, the script simulates a registered endpoint.</td>
</tr>
</tbody>
</table>

### Add a Registration Policy

You can add a custom registration policy to control registration by endpoints.

The policy can be applied to new registrations or to re-registrations from endpoints with changed properties.

Not all registration policies must be assigned to a port. A registration policy with no port assignment will be saved in your system but will not be used until you apply it to a port.

**Procedure**

1. Go to Service Config > Access Control > Registration Policies.
2. Click the Add button.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the registration policy.</td>
</tr>
<tr>
<td>Allow site-less registrations</td>
<td>When selected, endpoints that don't belong to a configured site or territory can register with the call server. Otherwise, only endpoints in a subnet configured in the site topology can register.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive registration deletion (days)</td>
<td>Select to specify that endpoints whose status is inactive (their registrations have expired) are deleted from the system after the specified number of days. Some dial rule actions, such as Resolve to registered endpoint, can route calls to endpoints with an inactive registration. To prevent this, you can delete inactive registration records or disable the Allow calls to inactive endpoints option in Call Server Settings.</td>
</tr>
<tr>
<td>Policy applies only to new devices</td>
<td>When selected, the system applies the registration policy only to new registrations from endpoints.</td>
</tr>
<tr>
<td>Policy applies to new or changed devices</td>
<td>When selected, the system applies the registration policy to new device registrations and also to re-registrations from changed endpoints (for example, an alias name change). You can optionally select Ignore IP and port changes so that the registration policy script is not applied if those are the only changes to an endpoint.</td>
</tr>
<tr>
<td>When compliant</td>
<td>Select the action to take when the registration policy script returns COMPLIANT.</td>
</tr>
<tr>
<td>When noncompliant</td>
<td>Select the action to take when the registration policy script returns NONCOMPLIANT.</td>
</tr>
<tr>
<td>Registration policy compliance script</td>
<td>The default compliance script for the Factory Core Registration Policy or the Factory Edge Registration Policy, depending on how you've configured your system. If you have a custom registration policy script, type (or paste) the script here.</td>
</tr>
</tbody>
</table>

4. Click Debug this Script to test the script with various dial strings and other variables (optional).
5. Click Cancel to close the Script Debugging window.
6. Click OK to close the Add Registration Policy window.
7. Click Reapply all policies to unblocked/unquarantined endpoints.

The system evaluates all unblocked and unquarantined endpoints and applies the registration policy that's associated with the last port through which an endpoint registered.

### Debug a Registration Policy Script

You can test and debug a registration policy script by using test values for the variables used in your script.

Testing your script is an iterative process. Repeat as often as necessary to see the results of applying your script using different variable values.

If necessary, make changes to your script and then test it again until it accomplishes what you intend.

**Procedure**

1. Go to Service Config > Access Control > Registration Policies.
2. Select the registration policy to debug.
3. Click the Edit button.
4. Under **Registration policy compliance script**, type (or paste) the registration policy script you want to debug.

5. Click **Debug this Script** to display the **Script Debugging** window.

6. Enter or select test values for the predefined variables.

7. Select **Is endpoint provisioned** to simulate a provisioned endpoint.

8. Select **Is endpoint registered** to simulate a registered endpoint.

9. Select an **Endpoint site** and **Subnet** to populate the site/subnet-related fields, which are read-only.

10. Click **Execute Script**.

    The **Script output** box displays any output produced by the script when it runs (for example, `println` statements and error messages). This output is recorded in the registration history. The **Script result** box displays the return value (COMPLIANT or NONCOMPLIANT) from running the script with the specified test values. If the script assigned a value to the EP_EXCEPTION variable, it displays that value.

### Edit a Registration Policy

You can edit registration policies, including the **Factory Core Registration Policy** and the **Factory Edge Registration Policy**.

**Procedure**

1. Go to **Service Config > Access Control > Registration Policies**.
2. Select the registration policy to edit.
3. Click the **Edit** button.
4. Revise the registration policy settings as needed.
5. Click **Debug this Script** to test the script with various dial strings and other variables (optional).
6. Click **Cancel** to close the **Script Debugging** window.
7. Click **OK** to close the **Edit Registration Policy** window.
8. Click **Apply policies to all endpoints**.

### Copy a Registration Policy

If you want to create a new registration policy that is similar to an existing one, you can copy the existing policy, rename it, and then revise it as needed.

**Procedure**

1. Go to **Service Config > Access Control > Registration Policies**.
2. Select the registration policy to copy.
3. Click the **Copy** button.
4. Enter a **Name** for the new registration policy.
5. Revise the other settings as needed.
6. Click **Debug this Script** to test the script with various dial strings and other variables.
7. Click **Cancel** to close the **Script Debugging** window.
8. Click **OK** to close the **Copy Registration Policy** window.
9. Click **Apply policies to all endpoints**.
Delete a Registration Policy

You can delete a registration policy, including the Factory Core Registration Policy and the Factory Edge Registration Policy, if the policy is not assigned to a port.

If a registration policy is assigned to a port, unassign it first before you delete it and assign a different registration policy to the port.

Procedure

1. Go to Service Config > Access Control > Registration Policies.
2. Select the registration policy to delete.
3. Click the Delete button.
4. Click Yes to confirm the deletion.

Assigning Registration Policies to Ports

A registration policy needs to be assigned to each public and private listening port for SIP and H.323 signaling.

The RealPresence DMA system applies the registration policy to every registration request that arrives on the port to which the registration policy is assigned.

You can assign only one registration policy per port but you can assign the same policy to multiple ports.

If you delete a port, the RealPresence DMA system assesses all endpoints and drops the registration of any endpoint that was last registered to the port you deleted. An endpoint whose registration is dropped must re-register to a new port.

The RealPresence DMA system has two default registration policies:

- The Factory Core Registration Policy is the default policy applied to SIP and H.323 listening ports on systems with a core configuration.
- The Factory Edge Registration Policy is the default policy applied to SIP and H.323 listening ports on systems with an edge configuration.

You can also assign a custom registration policy to a SIP or H.323 port.

Assign a Registration Policy to a SIP Port

You must assign a registration policy to each SIP listening port.

You can specify a custom registration policy or keep the default registration policy that's based on the system's configuration (core or edge).

Note: If you edit the registration policy assigned to a port during active calls, the calls may be disrupted or terminated.

Procedure

1. Go to Service Config > SIP Settings.
2. Select the port to assign the registration policy to and click the Edit button.
3. In the Registration policy field, select the policy to assign to the port.
4. Click OK.
Assign a Registration Policy to an H.323 Port

You must assign a registration policy to each H.323 listening port.

You can specify a custom registration policy or keep the default registration policy that's based on the system's configuration (core or edge).

**Note:** If you edit the registration policy assigned to a port during active calls, the calls may be disrupted or terminated.

**Procedure**

1. Go to Service Config > H.323 Settings.
2. In the Registration policy field, select the policy to assign to the port.
3. Click Update to save the settings.

**Sample Registration Policy Scripts**

A registration policy script is an executable script, written in the JavaScript language, that defines the criteria to be applied to registration requests in order to determine what to do with them.

For each request evaluated, the script must return **COMPLIANT** or **NONCOMPLIANT**.

The following sample scripts illustrate some of the ways in which registration requests can be evaluated. You can use them as templates or starting points for your scripts.

```javascript
// Reject endpoints with the specified problem software version and all SIP registrations. Record an appropriate exception for each case.

var result = COMPLIANT;
if (EP_VERSION == "1.2.3.4")
{
  EP_EXCEPTION += "Problem version 1.2.3.4 is not allowed\n";
  result = NONCOMPLIANT;
}
if (!EP_REG_IS_H323)
{
  EP_EXCEPTION += "SIP is not allowed\n";
  result = NONCOMPLIANT;
}
return result;

// Reject registration attempts by the SIPvicious SIP auditing tool
// (NOTE: typically this is used when DMA has public internet connectivity
// or in conjunction with the DMA Guest Port feature)

var result = COMPLIANT;
{
  EP_EXCEPTION += "SIPvicious is not allowed.";
  result = NONCOMPLIANT;
}
```
// This script illustrates how to integrate an existing registration policy script, such as the detection and blocking of penetration attacks like SIPVicious, with a policy that allows only endpoints with lower-case SIP URIs to register, while blocking registrations from endpoints whose SIP URIs contain upper case characters.

// The script only detects the conditions and returns "COMPLIANT" or "NONCOMPLIANT"; the registration policy can then be configured to block registrations from non-compliant endpoints.

// CAUTION: This script should be used in conjunction with a dial rule preliminary script that converts SIP dial strings that include upper case characters into dial strings with only lower case characters. See "Sample Registration Policy Scripts."

var result = COMPLIANT;
    EP_EXCEPTION += "SIPVicious is not allowed."
    result = NONCOMPLIANT;
}

// Include other registration policy checks above or below this script snippet, such as blocking penetration attacks like SIPvicious above.

var epssua = EP_SIP_SIP_URI_ALIAS + EP_SIP_SIPS_URI_ALIAS;
if (EP_REG_IS_SIP && epssua !== epssua.toLowerCase()) {
    result = NONCOMPLIANT;
    EP_EXCEPTION += "Noncompliant SIP Registration: Endpoint URI "+epssua + " contains upper-case letters."
}

return result;

// Reject aliases that aren't the right length; otherwise accept.

var CCAndAC = REG_SITE_COUNTRY_CODE + REG_SITE_AREA_CODE;
var DDlength = EP_H323_DIALEDDIGITS_ALIAS[0].length();
var SumDigits = parseInt(CCAndAC.length) + parseInt(REG_SITE_DIGITS);
if (DDlength > 0)
{
    if (DDlength != SumDigits) return NONCOMPLIANT;
}

// Reject aliases that aren't the right length; otherwise accept.
// Reject aliases that don't start with CC and AC (country code and area code);
// otherwise accept.
//
var CCAndAC = REG_SITE_COUNTRY_CODE + REG_SITE_AREA_CODE;
var DD_CCAndAC = EP_H323_DIALEDDIGITS_ALIAS[0] ?
EP_H323_DIALEDDIGITS_ALIAS[0].substring(0,CCAndAC.length) : "";
if (DD_CCAndAC != CCAndAC) return NONCOMPLIANT;

///////////////////////////////
// Reject aliases that don't start with AC (area code).
//
var AC = REG_SITE_AREA_CODE;
var DD_AC = EP_H323_DIALEDDIGITS_ALIAS[0].substring(0,AC.length);
var SIP_URI_AC = EP_SIP_TEL_URI_ALIAS.substring(0,AC.length);
if (DD_AC != AC) return NONCOMPLIANT;
if (SIP_URI_AC != AC) return NONCOMPLIANT;

///////////////////////////////
// A sample script that implements a whitelist of IP addresses for endpoints
// that can register.
// *** Note this does not take into account IPv6 addressing ***
//
var nparts;
var IPstring = "";
if (EP_IS_IPV4)
{
    IPstring = EP_IP.join(".");
}
for (i=0; i<whitelist.length; i++)
{
    if (IPstring.match(whitelist[i]))
    {
        return COMPLIANT;
    }
}
return NONCOMPLIANT;

///////////////////////////////
// A sample registration policy script with various combinations of blacklists
// and whitelists.
//
// Allows white/black listing of endpoints based on IP - Configure the
// IPOverride table below.
//
// Allows white/black listing of certain aliases - Configure the
// aliasOverride table below.
//
// Allows specific aliases to a given IP - Configure the allowAlias
// table below.
//
// An Override Action of "COMPLIANT" whitelists an IP or alias.
// An Override Action of "NONCOMPLIANT" blacklists an IP or alias.
//
// Notes:
IPOverride takes precedence over aliasOverride which takes precedence over the IP/Alias associations.

This script only works for IPv4 endpoints.

This script only works for H.323 endpoints that are registering with a single dialed-digits (E.164) alias.
- If it does not have dialed-digits alias or it has multiple dialed-digits aliases, the registration is not compliant.
- If it has a single dialed-digis alias AND other aliases, the registration is compliant if the dialed-digits alias is in the whitelist.

This script only works for SIP endpoints that are registering with a "sip:" URI alias. "sips:" and "tel:" aliases are not supported.

------BEGIN whitelist section------
Enter new lines with the format:
IPOverride["5.6.7.8"] = "Override Action";
var IPOverride = {};
IPOverride["5.6.7.9"] = "COMPLIANT";
IPOverride["8.8.8.8"] = "COMPLIANT";
IPOverride["40.242.225.50"] = "NONCOMPLIANT";
Enter new lines with the format:
aliasOverride["abcd"] = "Override Action";
var aliasOverride = {};
aliasOverride["999"] = "COMPLIANT";
aliasOverride["911"] = "COMPLIANT";
aliasOverride["12345678"] = "NONCOMPLIANT";
Enter new lines with the format:
allowAlias["A.B.C.D"] = "alias or SIP URI";
var allowAlias = {};
allowAlias["10.0.0.15"] = "1234";
allowAlias["172.20.10.5"] = "5678";
allowAlias["192.168.50.1"] = "john.doe@customer.com";
------END whitelist section------

---Variable definitions---
var IPAlias;
var IPstr = EP_IP[0];
var reg323Alias = EP_H323_DIALEDDIGITS_ALIAS;
var regSipAlias = EP_SIP_SIP_URI_ALIAS.toLowerCase();
---Step 1: EP_IP array is converted into a string for easier use.
for (var i = 1; i < 4; i++){
    IPstr += "." + EP_IP[i];
}
---Step 2: Check the IPOverride hash table to see if we should white/black
if(IPstr in IPOverride){
    return returnOverride(0,IPstr);
}
---Step 3: Handle SIP registrations. First, check if the SIP URI is white/black
if not, check to see if the IP has an allowed alias, and if the URI matches
the allowed alias.
// If none of the above, return NONCOMPLIANT.
else if(EP_REG_IS_SIP){
    if(regSipAlias in aliasOverride){
        return returnOverride(1, regSipAlias);
    }
    else if(IPstr in allowAlias){
        sAlias = allowAlias[IPstr];
        return checkAlias(regSipAlias, sAlias);
    } else{
        return NONCOMPLIANT
    }
}

//---Step 4: Handle H.323 registrations. First check if the alias is
// white/black listed.
// Next, reject registrations with more than 1 alias.
// Then, check if the IP has an allowed alias and check if the provided
// alias matches.
// If none of the above, return NONCOMPLIANT.
else if(EP_REG_IS_H323){
    if((reg323Alias[0] in aliasOverride) &&
        (typeof(reg323Alias[1])=='undefined')){
        return returnOverride(1, reg323Alias[0]);
    }
    else if(!(typeof(reg323Alias[1])=='undefined')){
        return NONCOMPLIANT;
    }
    else if (IPstr in allowAlias){
        hAlias = allowAlias[IPstr];
        return checkAlias(reg323Alias[0], hAlias);
    } else{
        return NONCOMPLIANT
    }
}

// Function definitions---//

// checkAlias function: Compares aliases from a registration and from the
// white
// list and returns the appropriate action.
function checkAlias(a0, aWl){
    if(a0 == aWl){
        return COMPLIANT;
    } else{
        return NONCOMPLIANT;
    }
}

// returnOverride function: ovrType is 0 (for IP) and 1 (for alias). Checks
// the
// ovrVal (IP or Alias) against the appropriate override list and returns
// the
// override action.
function returnOverride(ovrType, ovrVal){
    switch (ovrType) {
    case 0:
        return IPOverride[ovrVal];
        break;
    case 1:
        return aliasOverride[ovrVal];
        break;
Related Links

Registration Policy Scripting on page 396
Device Authentication

Topics:

- H.323 Device Authentication
- SIP Device Authentication
- Inbound Authentication
- Shared Outbound Authentication
- Add Device Authentication
- Edit Device Authentication

Device authentication enhances security by requiring devices registering with or calling the RealPresence DMA system to provide credentials that the system can authenticate.

In turn, the RealPresence DMA system may need to authenticate itself to an external SIP peer or gatekeeper.

All authentication configurations are supercluster-wide, but note that the default realm for SIP device authentication is the cluster’s domain as specified in Network Settings. This allows each cluster in a supercluster to have its own realm for challenges.

Related Links
Add an External SIP Peer on page 133
Edit an External SIP Peer on page 139
View External SIP Peers on page 132
Add an Authentication Credential Entry on page 151
Edit an Authentication Credential Entry on page 152
Add an External Gatekeeper on page 157
Edit an External Gatekeeper on page 159
Add an Endpoint on page 524
Edit Multiple Endpoints on page 526

H.323 Device Authentication

In an environment where H.235 authentication is used, H.323 devices include their credentials (name and password) in registration and signaling (RAS) requests.

The RealPresence DMA system authenticates requests as follows:

- If it's a signaling request (ARQ, BRQ, DRQ) from an unregistered endpoint, the call server doesn't authenticate the credentials.
- Otherwise, if the request is from an endpoint, an MCU, or neighbor gatekeeper, the call server attempts to authenticate using its device authentication list.
- If it's a signaling request from a registered endpoint, or if the request is from an MCU or neighbor gatekeeper, the call server attempts to authenticate using its device authentication list.
If the credentials can't be authenticated, the call server rejects the registration or signaling request. For call signaling requests, it also rejects the request if the credentials differ from those with which the device registered.

**SIP Device Authentication**

When a SIP endpoint registers with or calls the RealPresence DMA system, if the request includes authentication information, that information is checked against the call server's local device authentication list.

SIP authentication can be enabled at the port/transport level or (for unauthorized access prefixes) the prefix level.

If SIP authentication is enabled and an endpoint's request doesn't include authentication information, the call server responds with an authentication challenge containing the required fields. If the endpoint responds with valid authentication information, the system accepts the registration or call.

**Note:** If inbound SIP authentication is turned on for a port or prefix, the RealPresence DMA system challenges any SIP message coming to the system via that port or with that prefix. Any SIP peer and other device that interacts with the system by those means must be configured to authenticate itself, or you must turn off Device authentication for that specific device.

**Inbound Authentication**

In the Inbound Authentication section, you can configure specific SIP digest authentication settings for SIP devices.

You can also maintain the call server's local inbound device authentication list. This list is used for both H.235 authentication (H.323 devices) and SIP digest authentication (SIP devices).

**Shared Outbound Authentication**

In the Shared Outbound Authentication section, you can maintain the call server's general list of authentication credentials, which it uses to authenticate itself on behalf of calling devices to external SIP peers for which the appropriate device-specific credentials haven't been defined.

The call server intercepts and responds to authentication challenges from SIP peers on behalf of some or all devices calling through the call server. This feature allows authentication security between the call server and its peers to be completely separate from security between the endpoints and the call server.

When you add an external SIP peer, you can specify whether the call server handles challenges (401 and 407) on behalf of the source of the call or passes them on to the source of the call. You can also define authentication credentials specifically for that SIP peer.

**Note:** For H.323, when you add an external neighbor gatekeeper, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.

The following table describes the fields on the Device Authentication page.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbound Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>SIP device authentication settings</td>
<td>This option, the default, sets the realm for the call server to the cluster's domain as specified on the <strong>Network Settings</strong> page (allowing each cluster of a supercluster to have its own realm). If no domain is specified on the <strong>Network Settings</strong> page, the default realm value is <code>sip.dma</code>. Clear the check box to change the string in the <strong>Realm</strong> field.</td>
</tr>
<tr>
<td>Realm</td>
<td>The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally, it includes the domain label of the call server. See RFC 2617 and RFC 3261. If you specify a realm instead of using the default, the realm you specify is used for all clusters in the supercluster.</td>
</tr>
<tr>
<td>Enable proxy authentication</td>
<td>Configures the call server to respond to unauthenticated requests with 407 (Proxy Authentication Required). If turned off, the call server responds to unauthenticated requests with 401 (Unauthorized).</td>
</tr>
<tr>
<td>Authentication valid time (seconds)</td>
<td>Specifies the time period within which the call server doesn't re-challenge a device that previously authenticated itself.</td>
</tr>
<tr>
<td><strong>Inbound Device Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>(List of authentication entries)</td>
<td>Lists the inbound device authentication entries. The call server checks a device's credentials against these entries.</td>
</tr>
<tr>
<td><strong>Shared Outbound Authentication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Outbound Device Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>(List of authentication entries)</td>
<td>Lists the authentication credential entries defined for general use by the call server to authenticate its requests, showing the realm in which the entry is valid and the user name. You can add, edit, or delete credential entries. Use the <strong>Realm</strong> or <strong>Name</strong> field and <strong>Search</strong> button above the list to narrow the list. When choosing authentication credentials to present to an external SIP peer, the call server looks first for an appropriate entry specific to that SIP peer. If there is none with the correct realm, it looks at the entries listed here.</td>
</tr>
</tbody>
</table>
Add Device Authentication

You can add a device's authentication credentials to the list of entries against which the call server checks device credentials.

Procedure

1. Go to Service Config > Access Control > Device Authentication.
2. Select the Add button.
3. In Add Device Authentication Credentials, complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Authentication Name | The name that the device includes in registration and signaling requests or responses to authentication challenges.  
**Note:** The name and password for a device are whatever values the person who configured the device specified. They don't uniquely identify a specific device; multiple devices can have the same name and password. |
| Password          | The password that the device includes in registration and signaling requests or responses to authentication challenges.                        |
| Confirm password  |                                                                                                                                            |

Edit Device Authentication

You can edit a selected device's authentication credentials as needed.

Procedure

1. Go to Service Config > Access Control > Device Authentication.
2. Select the device to edit.
3. Click the Edit icon.
4. In Edit Device Authentication Credentials, revise the fields as described in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Authentication Name | The name that the device includes in registration and signaling requests or responses to authentication challenges.  
**Note:** The name and password for a device are whatever values the person who configured it specified. They don't uniquely identify a specific device; multiple devices can have the same name and password. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password that the device includes in registration and signaling requests or responses to authentication challenges.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>
Site Topology

Topics:

- Site Topology
- Working with Site Topology

This section provides information on site topologies.
Site Topology

Topics:

- Shared Site Topology for Integrated Polycom Systems
- Bandwidth Management
- Cascade for Bandwidth Conferences
- Supercluster Assignments
- Configure Site Topology
- Embedded DNS

Within your Polycom environment, both the RealPresence Resource Manager system and RealPresence DMA systems require a site topology to be configured.

If your environment includes integrated RealPresence Resource Manager and RealPresence DMA systems, you must use the RealPresence Resource Manager system to manage the site topology. When integrated with a RealPresence Resource Manager system, the RealPresence DMA system inherits all site topology and the settings within the RealPresence DMA system are read-only.

Site topology information logically describes your network and its interfaces to other networks, including the following elements:

- **Site** - A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device's IP address identifies the site to which it belongs.

- **Network cloud** - A multiprotocol label switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and Quality of Service (QoS) information.

- **Site link** - A network connection between two sites or between a site and an MPLS network cloud.

- **Site-to-site exclusion** - A site-to-site connection that the site topology doesn’t permit a voice or video call to use.

- **Territory** - A collection of one or more sites for which a RealPresence DMA cluster is responsible. Territories serve multiple purposes in a RealPresence DMA system deployment.

The system installs with a default site topology with sites, subnets, and a site link that allow for endpoint registration and call routing (both multipoint and point-to-point).

Site topology information provides a logical model representation of a network topology, not necessarily a fully accurate literal representation of a full network.

Related Links

[Organize Territories and Assign Responsibilities](#) on page 126
Shared Site Topology for Integrated Polycom Systems

If you have integrated a RealPresence Resource Manager system with a RealPresence DMA system, you must use the RealPresence Resource Manager system to manage the site topology.

When integrated with a RealPresence Resource Manager system, the RealPresence DMA system inherits all site topology settings.

Bandwidth Management

Once you model a site topology to represent your physical network, you can use it to manage bandwidth between your sites, preventing conference traffic from saturating the network.

Before the RealPresence DMA system routes a call, it considers the source and destination IP addresses in the site topology and determines a media path from the source subnet to the destination subnet, taking into account the existing calls and bandwidth restrictions along that path. If sites or site links have bandwidth restrictions, the system reduces the call rate of the call at the time of call setup so that it meets those restrictions, if possible. If the media path is already saturated with other conference traffic, the RealPresence DMA system rejects the call attempt.

Cascade for Bandwidth Conferences

For a conference with cascading for bandwidth enabled, the RealPresence DMA system uses the site topology information to route calls to the nearest eligible MCU (based on pools and pool orders) that has available capacity and to create the cascade links between MCUs.

Cascading for bandwidth uses a hub-and-spoke configuration so that each cascaded MCU is only one link away from the hub MCU, which hosts the conference. The conference is hosted on the same MCU that would have been chosen in the absence of cascading, using the pool order applicable to the conference.

The cascade links between MCUs must use H.323 signaling. For conferences with cascading enabled, the RealPresence DMA system selects only MCUs that have H.323 signaling enabled.

This cascade link requirement doesn't affect endpoints, which may dial in using SIP (assuming the MCUs and the RealPresence DMA system are also configured for SIP signaling).

Supercluster Assignments

Within a RealPresence DMA system, cluster responsibility is determined via the site topology.

If your RealPresence DMA system is superclustered, site topology data only needs to be created (or obtained from a RealPresence Resource Manager system) on one cluster of the superclusters. The data is replicated across the supercluster.
Configure Site Topology

You can configure your site topology in the RealPresence DMA system.

For a conference with cascading for bandwidth enabled, the RealPresence DMA system routes calls to the nearest eligible MCU (based on pools and pool orders) that has available capacity and to create the cascade links between MCUs.

If you integrate this system with a RealPresence Resource Manager system, the site topology information from the RealPresence Resource Manager system will replace the information you entered.

Procedure

1. Go to Service Config > Site Topology > Network Clouds.
2. For each site in your network topology, do the following:
   a. Click the Add button.
   b. In the Add Site dialog, complete the General Info section.
   c. To enable IP calls to and from the site, complete the ISDN Number Assignment, H.323 Routing and/or SIP Routing sections.
   d. In the Subnets section, specify the subnet or subnets that make up the site.
   e. Click OK.
3. Go to Service Config > Site Topology > Territories.
   The list of territories contains an entry named Default RealPresence DMA Territory. It's assigned to this RealPresence DMA system cluster. You can edit this entry, including changing its name and assigning sites to it.
4. Edit the Default RealPresence DMA Territory entry:
   a. Select the entry and, in the Actions list, click Edit.
      The Edit Territory dialog appears.
   b. In the Territory Info section, change the name and description for this territory if desired.
      Assign a primary and backup cluster for the territory, and elect whether to host conference rooms in this territory (the primary and backup cluster must be licensed for this capability).
   c. In the Associated Sites section, add all the sites to the territory.
   d. Click OK.
5. Add other territories by clicking Add in the Actions list and completing the same settings in the Add Territory dialog.
6. Go to Service Config > Site Topology > Site Links, and for each direct link between sites, do the following:
   a. In the Actions list, click Add.
   b. In the Add Site Link dialog, define the link.
   c. Click OK.
7. Go to Service Config > Site Topology > Network Clouds, and for each MPLS network cloud in your network topology, do the following:
   a. In the Actions list, click Add.
      The Add Network Cloud dialog appears.
b. In the **Cloud Info** section, enter a name and description for the cloud.

c. In the **Linked Sites** section, display the sites you defined.

d. Select the first site linked to this cloud and click the arrow button to move it to the **Linked Sites** list.

   The **Add Site Link** dialog appears.

e. Define the link.

f. Repeat the previous two steps for each additional site linked to this cloud.

g. Click **OK**.

8. Go to **Service Config > Site Topology > Site-to-Site Exclusions**, and for each exclusion in your network topology, do the following:

   a. In the **Actions** list, click **Add**.

   b. Complete the **Add Site-to-Site Exclusions** wizard.

### Embedded DNS

In a superclustered configuration, the clusters that make up the supercluster automatically take over for each other in the event of an outage.

In order to gain the full benefit of this feature, however, the endpoints that are registered to each cluster must re-register to a new cluster when the new cluster takes over.

This can be accomplished by specifying the gatekeeper or SIP proxy that each endpoint will register to as a site's domain name, rather than an IP address. Then, when there is a failover, the DNS A record for that site's domain name can be mapped to a different IP address, changing the call server that each endpoint is registered to.

The embedded DNS capability of the RealPresence DMA system automates this procedure.

Each RealPresence DMA server hosts its own embedded DNS server. It publishes a DNS CNAME record for each site. That CNAME record maps to the active cluster with which endpoints at the site should register. Whenever responsibility for the site moves from one cluster to another, the change is automatically published by the embedded DNS server. Endpoints will automatically re-register to the correct cluster.

You can enable these embedded DNS servers on the **Embedded DNS** page. This is a supercluster-wide setting.

Embedded DNS is enabled by default for newly installed RealPresence DMA systems. In its default configuration, the **Call server sub-domain controlled by DMA system** field is populated with the default sub-domain `video.local`. The system acts as an initial DNS server, resolving the FQDN `dma.video.local` to the virtual IPv4 address of the local cluster. If you change the sub-domain to a custom value, the embedded DNS service resolves `dma.<newsubdomain>` to the IP address of the cluster.

To use this feature, your enterprise DNS must place the RealPresence DMA supercluster in charge of resolving the sub-domain `video.local`. To do this, you must:

- Add NS records to your enterprise DNS so that it refers requests to resolve the site-based logical host name to the embedded DNS servers.
- Configure your enterprise DNS to forward requests for names in the site-based logical host name to any of the clusters in the supercluster.

Embedded DNS functionality is not supported in an IPv6 environment.

The following table describes the fields on the Embedded DNS page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable embedded DNS service</td>
<td>Enables the embedded DNS servers.</td>
</tr>
<tr>
<td>Call server sub-domain controlled by DMA</td>
<td>The fully qualified domain name of the enterprise domain for which the RealPresence DMA system will provide DNS. For instance, for the base domain example.com, the sub-domain that the RealPresence DMA system services might be:</td>
</tr>
<tr>
<td></td>
<td>callservers.example.com</td>
</tr>
<tr>
<td></td>
<td>This is the logical call server domain name for which you must create NS records in your enterprise DNS. And this is the domain name that the system combines with each site name to form the logical FQDN that endpoints in each site should register to.</td>
</tr>
</tbody>
</table>

Related Links
- View the Site Information on page 421
- Add a Site on page 422
- Edit a Site on page 428

Enable DNS Publishing

You can enable embedded DNS publishing on the Embedded DNS page.

If you have a RealPresence Resource Manager system integrated with the RealPresence DMA system, select Support DMA Supercluster on the Edit DMA page and enter all network/DNS-related information in lowercase.

Procedure
1. Be sure you've added the required NS records, one for each cluster in the supercluster, to your enterprise DNS and have configured it to forward requests for names in the logical call server domain to any of the clusters in the supercluster.
2. Go to Service Config > Embedded DNS.
3. Click Enable embedded DNS service.
4. In the Call server sub-domain controlled by DMA field, enter the logical call server domain name (the enterprise domain for which the RealPresence DMA system will provide DNS) and click Update.
5. Reconfigure your endpoints to register to the correct domain name for their site.
To determine the correct domain name for a site, go to Service Config > Site Topology > Sites, select the site, and click Site Information. The Logical host name field displays the correct domain name. It takes the form:

```
callserver-<site name>.<logical call server domain name>
```

For example, if the fully qualified domain name for the logical call server domain is callservers.example.com, the correct domain name for endpoints in the paris site is:

```
callserver-paris.callservers.example.com
```
Working with Site Topology

Topics:

- Sites
- Network Clouds
- Site Links
- Site-to-Site Exclusions
- Territories

If you've integrated a RealPresence Resource Manager system with a RealPresence DMA system, the system inherits all site topology settings from the RealPresence Resource Manager system and you must use the RealPresence Resource Manager system to manage the site topology.

You can't edit site topology information from the RealPresence DMA system. If the RealPresence DMA system is not integrated, you can enter site information from its web user interface.

Sites

The Internet/VPN and Default Site entries are provided with a new installation of the RealPresence DMA system.

The Internet/VPN entry always exists and cannot be edited or deleted. It cannot be assigned to a territory or controlled by a cluster. Endpoints whose subnet is not in any defined site in the enterprise network are considered to be in the Internet/VPN site. They can register to a cluster only if site-less registrations are allowed.

The Default Site entry has no restrictions. This site is configured to route SIP calls through a SIP-aware firewall, and includes three subnets that together cover the private IPv4 address space.

The protocol-specific routing settings for a site determine whether and how calls from that site can traverse the firewall to reach endpoints outside the enterprise network in one of the following ways:

- Through a transparent firewall
- Through the specified session border controller (SBC)
- Not at all

The site's routing settings are used when the dial string is resolved by a dial rule using the Resolve to external address or Resolve to IP address action.

Alternatively, you can add an H.323 SBC or an external SIP peer that can only be reached by dialing a specific prefix or prefixes. A dial string beginning with such a prefix can be resolved by the dial rule using the Resolve to service prefix action.

View the Site List

You can view a list of sites within your system’s site topology.

Procedure

» Go to Service Config > Site Topology > Sites.
The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Note:</td>
<td>When the embedded DNS feature is enabled, site names are limited to 52 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the site.</td>
</tr>
<tr>
<td>Country code</td>
<td>The country code for the site's location.</td>
</tr>
<tr>
<td>Area code</td>
<td>The city or area code for the site's location.</td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the site belongs, which determines the RealPresence DMA cluster responsible for it.</td>
</tr>
</tbody>
</table>

**View the Site Information**

You can view information about the selected site, including which subnets are associated with it and counts of the devices it contains.

**Procedure**

1. Go to Service Config > Site Topology > Sites.
2. Select the site with the detailed information you want to view.
3. Select Site Information.

The following table describes the fields in the Site Information window. The information is read-only.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Info</td>
<td></td>
</tr>
<tr>
<td>Site name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>If the system's embedded DNS service is enabled, the system uses the site name to create the Logical host name (see below). Naming recommendations:</td>
<td></td>
</tr>
<tr>
<td>• Use site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens).</td>
<td></td>
</tr>
<tr>
<td>• Enter network/DNS - related information in all lowercase to avoid possible case-sensitivity issues with various devices and ensure interoperability.</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the site.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logical host name</td>
<td>If the system's embedded DNS service is enabled, this is the logical FQDN that endpoints in this site should register to. The system generates this by combining callserver, the site name, and the value specified in the Call server sub-domain controlled by RealPresence DMA field on the Embedded DNS page. If the site name contains a character not permitted in a host name, the system replaces it with a dash (hyphen) followed by the hex code of the ASCII character. For example, if the site is named paris (north) and the call server sub-domain is callservers.example.com, the logical host name would be: callserver-paris-20-28north-29.callservers.example.com</td>
</tr>
</tbody>
</table>

### Device Types

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCUs</td>
<td>The number of MCUs in the site.</td>
</tr>
<tr>
<td>DMAs</td>
<td>The number of RealPresence DMA systems in the site.</td>
</tr>
<tr>
<td>VBPs</td>
<td>The number of Polycom Video Border Proxy NAT/firewall traversal appliances in the site.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>The number of registered endpoints in the site.</td>
</tr>
<tr>
<td>Subnets</td>
<td>A list of the subnets in the site.</td>
</tr>
</tbody>
</table>

### Related Links

- [DNS Records for the RealPresence DMA System](#) on page 48
- [Embedded DNS](#) on page 417
- [Call Server Settings](#) on page 297

### Add a Site

You can define a new site in the RealPresence DMA system's site topology and specify which subnets are associated with the site.

**Note:** Enter all network/DNS-related information in all lowercase to avoid possible case-sensitivity issues with various devices and ensure interoperability.

**Procedure**

1. Go to Service Config > Site Topology > Sites.
2. Click the Add button.
3. Complete the fields as described in the following table:
## General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site name</td>
<td>A meaningful name for the site (up to 128 characters). <strong>Note:</strong> If the system's embedded DNS service is enabled, the system uses the site name to create the Logical host name. Polycom recommends:</td>
</tr>
<tr>
<td></td>
<td>• Using site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens).</td>
</tr>
<tr>
<td></td>
<td>• Entering network/DNS-related information in all lowercase to avoid possible case-sensitivity issues with various devices and ensure interoperability.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the site (up to 200 characters).</td>
</tr>
</tbody>
</table>

## Bandwidth Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth.</td>
</tr>
<tr>
<td></td>
<td>This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. <strong>Note:</strong> When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

## Territory Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territory</td>
<td>Assigns the site to a territory, and thus to a RealPresence DMA cluster.</td>
</tr>
</tbody>
</table>
### ISDN Number Assignment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assignment method    | The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the call server and ISDN endpoints dialing in through an ISDN gateway. The assignment options are:  
  • **No assignment** - Select this option when you don't want to define a range of E.164 aliases for the site.  
  • **Manual assignment** - Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.  
  • **Automatic assignment** - Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias. After an E.164 alias is assigned to an endpoint, it's reserved for use as long as that endpoint remains registered with the RealPresence DMA system.  
  
  If you do not enable **Automatic assignment**, you can manually add E.164 aliases to endpoints. And endpoints will have any aliases with which they register. |
| Dialing method       | The ISDN inward dialing method for the site:  
  • **DID (Direct Inward Dial)** - Select this option if your ISDN gateway is provisioned with a range of phone numbers from the ISDN service provider, and each of these numbers will be assigned to an endpoint as an alias.  
  • **Gateway Extension Dialing** - Select this option if your ISDN gateway's ISDN connection is provisioned with a single gateway phone number from the ISDN service provider, and endpoints will be assigned an extension (E.164 alias) that's internal to the company and doesn't correspond to any number that can be dialed on the PSTN. Endpoints can be dialed from the PSTN by dialing the ISDN gateway phone number, followed by a delimiter (usually a #) and the extension number. The gateway receives the full number from the PSTN and dials only the extension number on the IP network. |
### ISDN Outbound Dialing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override ITU dialing rules</td>
<td>Check this box to override the standard dialing rules, established by the International Telecommunications Union (ITU), when dialing out using an ISDN gateway. The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.</td>
</tr>
<tr>
<td>PBX access code</td>
<td>The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.</td>
</tr>
<tr>
<td>Country code</td>
<td>The country code for the site's location. Click the CC button to select from a list of countries. To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call's destination.</td>
</tr>
<tr>
<td>Area code</td>
<td>The city or area code for the site's location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field. To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call's destination.</td>
</tr>
<tr>
<td>Always dial area code</td>
<td>Specifies that the area code should always be included in the phone number.</td>
</tr>
<tr>
<td>Always dial national prefix</td>
<td>Specifies that the national prefix should always be included in the phone number.</td>
</tr>
<tr>
<td>Length of subscriber number</td>
<td>The number of digits in a phone number. For example, in the United States and other areas using the North American Numbering Plan (NANP), subscriber numbers have seven digits.</td>
</tr>
</tbody>
</table>

### ISDN Range Assignment (for DID dialing method)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length of call line identifier</td>
<td>The number of digits in the call line identifier (CLID), which is the dialed number. The maximum is 17. For example, in the United States, the number of digits in the CLID is often 7 for outside local calls and 11 for callers in a different area code.</td>
</tr>
<tr>
<td>Length of short phone number</td>
<td>The number of digits in the short form of the dialing number. For example, in the United States, internal extensions are usually four or five digits.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISDN number ranges</td>
<td>The number ranges available for assignment to endpoints in the site. Click <strong>Add</strong> to add a new range of numbers. Click <strong>Edit</strong> or <strong>Delete</strong> to change or delete the selected range. The start and end numbers in the range should be entered with the same number of digits. If the range is 303-223-1000 to 1999, enter 3032231000 and 3032231999.</td>
</tr>
<tr>
<td>ISDN gateway number</td>
<td>An ISDN gateway phone number for the site. This field is just for your reference. It's not used by the software to process calls. If the site has more than one ISDN gateway, you'll need to know their access numbers and determine how to instruct inbound users to call.</td>
</tr>
<tr>
<td>E.164 start</td>
<td>The beginning of the range of E.164 extensions associated with the site.</td>
</tr>
<tr>
<td>E.164 end</td>
<td>The end of the range of E.164 extensions associated with the site. The start and end numbers in the range should be entered with the same number of digits.</td>
</tr>
<tr>
<td>H.323 Routing</td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables H.323 calls to the internet.</td>
</tr>
<tr>
<td>Allowed via H.323-aware firewall</td>
<td>Allows H.323 calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Allowed via H.323-aware SBC or ALG</td>
<td>Enables H.323 calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td>SIP Routing</td>
<td></td>
</tr>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables SIP calls to the internet.</td>
</tr>
<tr>
<td>Allowed via SIP-aware firewall</td>
<td>Enables calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Allowed via SIP-aware SBC or ALG</td>
<td>Enables SIP calls to the internet through the specified SBC or ALG.</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the SBC or ALG.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Lists the subnets in the site. Click <strong>Add</strong> to add a subnet. Select a subnet in the table and click <strong>Edit</strong> or <strong>Delete</strong> to modify or remove it.</td>
</tr>
<tr>
<td>Name</td>
<td>The unique name of the subnet.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the subnet.</td>
</tr>
<tr>
<td></td>
<td>You can define overlapping subnets; larger subnets can contain smaller ones. When the system determines which subnet a given IP address belongs to, it chooses the subnet with the longest IP address match. For example:</td>
</tr>
</tbody>
</table>
|       | subnet1 = 10.0.0.0/8  
|       | subnet2 = 10.33.24.0/24  
|       | The IP address 10.33.24.70 belongs to **subnet2**. The IP address 10.22.23.70 belongs to **subnet1**. |
| Subnet mask length | The classless inter-domain routing (CIDR) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the **IP Address**, defines the subnet. |
|       | For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a subnet mask of 255.255.0.0. |
|       | You can use subnet mask lengths of up to 32 bits; a 32-bit subnet mask allows you to specify a single device. |
| Max total bandwidth (Mbps) | When selected, you can specify the total bandwidth limit for voice and video calls. |
| Max per-call bit rate (kbps) | The per-call bit rate limit for voice and video calls. |
|       | When you specify both the bandwidth and bit rate limits, the **Add Site** window displays how many calls at that bit rate the specified bandwidth limit supports. The value of the **Bit rate to bandwidth conversion factor** on the **Call Server Settings** page is used in this calculation. |
| Max per-call custom bit rate (kbps) | The customized per-call bit rate limit for voice and video calls. |

4. Click **OK** to add the site.

**Related Links**
- [Call Server Settings](#) on page 297
- [Embedded DNS](#) on page 417
Edit a Site

You can edit a site in the RealPresence DMA system's site topology and add or edit a subnet associated with the site.

**Note:** Enter all network/DNS-related information in all lowercase to avoid possible case-sensitivity issues with various devices and ensure interoperability.

**Procedure**

1. Go to **Service Config > Site Topology > Sites**.
2. Choose a site from the list, and click the **Edit** button.
3. Complete or revise the fields as described in the following table:

### General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site name</td>
<td>A meaningful name for the site (up to 128 characters).</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If the system's embedded DNS service is enabled, the system uses the site name to create the Logical host name Polycom recommends:</td>
</tr>
<tr>
<td></td>
<td>• Using site names that contain only characters permitted in a host name (letters, numbers, and internal hyphens).</td>
</tr>
<tr>
<td></td>
<td>• Entering network/DNS-related information in all lowercase to avoid possible case-sensitivity issues with various devices and ensure interoperability.</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the site (up to 200 characters).</td>
</tr>
</tbody>
</table>

### Bandwidth Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth. This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth limit supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>
### Territory Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territory</td>
<td>Assigns the site to a territory, and thus to a RealPresence DMA cluster.</td>
</tr>
</tbody>
</table>

### ISDN Number Assignment

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assignment method | The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the call server and ISDN endpoints dialing in through an ISDN gateway. The assignment options are:  
  - **No assignment** - Select this option when you don't want to define a range of E.164 aliases for the site.  
  - **Manual assignment** - Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.  
  - **Automatic assignment** - Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias.  
  
  After an E.164 alias is assigned to an endpoint, it’s reserved for use as long as that endpoint remains registered with the RealPresence DMA system.  
  
  If you do not enable **Automatic assignment**, you can manually add E.164 aliases to endpoints. And endpoints will have any aliases with which they register. |
| Dialing method   | The ISDN inward dialing method for the site:  
  - **DID (Direct Inward Dial)** - Select this option if your ISDN gateway is provisioned with a range of phone numbers from the ISDN service provider, and each of these numbers will be assigned to an endpoint as an alias.  
  - **Gateway Extension Dialing** - Select this option if your ISDN gateway's ISDN connection is provisioned with a single gateway phone number from the ISDN service provider, and endpoints will be assigned an extension (E.164 alias) that's internal to the company and doesn't correspond to any number that can be dialed on the PSTN.  
  
  Endpoints can be dialed from the PSTN by dialing the ISDN gateway phone number, followed by a delimiter (usually a #) and the extension number. The gateway receives the full number from the PSTN and dials only the extension number on the IP network. |
### ISDN Outbound Dialing

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override ITU dialing rules</td>
<td>Check this box to override the standard dialing rules, established by the International Telecommunications Union (ITU), when dialing out using an ISDN gateway. The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.</td>
</tr>
<tr>
<td>PBX access code</td>
<td>The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.</td>
</tr>
<tr>
<td>Country code</td>
<td>The country code for the site's location. Click the CC button to select from a list of countries. To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call's destination.</td>
</tr>
<tr>
<td>Area code</td>
<td>The city or area code for the site's location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field. To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call's destination.</td>
</tr>
<tr>
<td>Always dial area code</td>
<td>Specifies that the area code should always be included in the phone number.</td>
</tr>
<tr>
<td>Always dial national prefix</td>
<td>Specifies that the national prefix should always be included in the phone number.</td>
</tr>
<tr>
<td>Length of subscriber number</td>
<td>The number of digits in a phone number. For example, in the United States and other areas using the North American Numbering Plan (NANP), subscriber numbers have seven digits.</td>
</tr>
</tbody>
</table>

### ISDN Range Assignment (for DID dialing method)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length of call line identifier</td>
<td>The number of digits in the call line identifier (CLID), which is the dialed number. The maximum is 17. For example, in the United States, the number of digits in the CLID is often 7 for outside local calls and 11 for callers in a different area code.</td>
</tr>
<tr>
<td>Length of short phone number</td>
<td>The number of digits in the short form of the dialing number. For example, in the United States, internal extensions are usually four or five digits.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ISDN number ranges</td>
<td>The number ranges available for assignment to endpoints in the site. Click <strong>Add</strong> to add a new range of numbers. Click <strong>Edit</strong> or <strong>Delete</strong> to change or delete the selected range. The start and end numbers in the range should be entered with the same number of digits. If the range is 303-223-1000 to 1999, enter 3032231000 and 3032231999.</td>
</tr>
</tbody>
</table>

**ISDN Range Assignment (for gateway extension dialing method)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN gateway number</td>
<td>An ISDN gateway phone number for the site. This field is just for your reference. It's not used by the software to process calls. If the site has more than one ISDN gateway, you'll need to know their access numbers and determine how to instruct inbound users to call.</td>
</tr>
<tr>
<td>E.164 start</td>
<td>The beginning of the range of E.164 extensions associated with the site.</td>
</tr>
<tr>
<td>E.164 end</td>
<td>The end of the range of E.164 extensions associated with the site. The start and end numbers in the range should be entered with the same number of digits.</td>
</tr>
</tbody>
</table>

**H.323 Routing**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables H.323 calls to the internet.</td>
</tr>
<tr>
<td>Allowed via H.323-aware firewall</td>
<td>Allows H.323 calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Allowed via H.323-aware SBC or ALG</td>
<td>Enables H.323 calls to the internet through the specified session border controller (SBC) or application layer gateway (ALG).</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the H.323 SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the H.323 SBC or ALG.</td>
</tr>
</tbody>
</table>

**SIP Routing**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet calls are not allowed</td>
<td>Disables SIP calls to the internet.</td>
</tr>
<tr>
<td>Allowed via SIP-aware firewall</td>
<td>Enables calls to the internet through a firewall.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allowed via SIP-aware SBC or ALG</td>
<td>Enables SIP calls to the internet through the specified SBC or ALG.</td>
</tr>
<tr>
<td>Call signaling address (IPv4)</td>
<td>The call signaling address for the SBC or ALG.</td>
</tr>
<tr>
<td>Port</td>
<td>The call signaling port for the SBC or ALG.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Lists the subnets in the site. Click Add to add a subnet. Select a subnet in the table and click Edit or Delete to modify or remove it.</td>
</tr>
<tr>
<td>Name</td>
<td>The unique name of the subnet.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the subnet.</td>
</tr>
<tr>
<td></td>
<td>You can define overlapping subnets; larger subnets can contain smaller ones. When the system determines which subnet a given IP address belongs to, it chooses the subnet with the longest IP address match. For example:</td>
</tr>
</tbody>
</table>
|                                  | ```subnet1 = 10.0.0.0/8```  
|                                  | ```subnet2 = 10.33.24.0/24```  
|                                  | The IP address 10.33.24.70 belongs to subnet2. The IP address 10.22.23.70 belongs to subnet1. |
| Subnet mask length               | The classless inter-domain routing (CIDR) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the IP Address, defines the subnet. For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a subnet mask of 255.255.0.0. You can use subnet mask lengths of up to 32 bits; a 32-bit subnet mask allows you to specify a single device. |
| Max total bandwidth (Mbps)       | When selected, you can specify the total bandwidth limit for voice and video calls. |
| Max per-call bit rate (kbps)     | The per-call bit rate limit for voice and video calls. When you specify both the bandwidth and bit rate limits, the Add Site window displays how many calls at that bit rate the specified bandwidth limit supports. The value of the Bit rate to bandwidth conversion factor on the Call Server Settings page is used in this calculation. |
| Max per-call custom bit rate (kbps) | The customized per-call bit rate limit for voice and video calls. |

4. Click **OK**.

**Related Links**
- [External SIP Peers](#) on page 131
- [Call Server Settings](#) on page 297
- [Embedded DNS](#) on page 417
**Add a Subnet**

When you add or edit a site, you can add subnets to the site.

You can’t assign the same subnet to more than one site.

If you have an edge system in H.323 routed call mode communicating with a core system in H.323 direct call mode and you make outbound calls from endpoints registered to the core system to endpoints registered to the edge system (or guest endpoints) on the Internet, you need to add a subnet to the edge system’s Default Site that includes all the endpoints registered to the core system.

A newly installed edge system doesn’t have any subnets defined in the Default Site. After installation, you can run the DMA Edge Wizard to configure your edge system. The wizard adds the core system’s Core DMA Subnet of registered endpoints to the edge system’s Default Site. If you don’t use the wizard, you can manually add the subnet.

**Procedure**

1. Go to **Service Config > Site Topology > Sites**.
2. Click **Add** to add a new site, or **Edit** to edit an existing site.
3. In the **Add Site** or **Edit Site** dialog, select the **Subnets** section.
4. Click **Add**.
5. In the **Add Subnet** window, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the subnet. Required and must be unique.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the subnet.</td>
</tr>
<tr>
<td>Subnet mask length</td>
<td>The classless inter-domain routing (CIDR) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the IP address, defines the subnet. For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a dotted-quad subnet mask of 255.255.0.0.</td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls. If not specified, the site limit applies.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls. If not specified, the site limit applies. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth supports. The value of the <strong>Bit rate to bandwidth conversion factor</strong> setting on the <strong>Call Server</strong> Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

6. Click **OK**.

**Related Links**

[Call Server Settings](#) on page 297
Edit a Subnet

You can edit a subnet associated with a site.

You cannot assign the same subnet to more than one site.

Procedure

1. Go to Service Config > Site Topology > Sites.
2. Choose a site from the list, and click Edit.
3. In the Edit Site window, select the Subnets section.
4. Click Edit.
5. In the Edit Subnet window, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the subnet. Required and must be unique.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the subnet.</td>
</tr>
</tbody>
</table>
| Subnet mask length  | The classless inter-domain routing (CIDR) prefix size value (the number of leading 1 bits in the routing prefix mask). This value, together with the IP Address, defines the subnet. 
For IPv4, a value of 24 is equivalent to specifying a dotted-quad subnet mask of 255.255.255.0. A value of 16 is equivalent to specifying a subnet mask of 255.255.0.0. |
| Max total bandwidth (Mbps) | The total bandwidth limit for voice and video calls. If not specified, the site limit applies.                                                   |
| Max per-call bit rate (kbps) | The per-call bit rate limit for voice and video calls. If not specified, the site limit applies.                                                |
|                     | When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation. |

6. Click OK.

Related Links

Call Server Settings on page 297

Network Clouds

You can define multiprotocol label switching (MPLS) network clouds in your site topology.

MPLS is a special technology typically offered via a private WAN environment, providing more reliability than the Internet. If you're unsure if your enterprise has an MPLS network cloud, speak to your IT administrator.

If the RealPresence DMA system is integrated with a RealPresence Resource Manager system, it receives MPLS network information from that system, and this page is read-only. If not, you can enter MPLS network cloud information.
View Network Clouds
You can view a list of any network clouds you have added.

Procedure
  » Go to Service Config > Site Topology > Network Clouds.
    The network cloud lists each cloud by name and description.

Add a Network Cloud
You can define a new MPLS network cloud in your system's site topology.

Procedure
  1. Go to Service Config > Site Topology > Network Clouds.
  2. In the Actions list, click Add.
  3. In the Add Network Cloud dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Info</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the cloud (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the cloud (up to 200 characters).</td>
</tr>
<tr>
<td>Associated Sites</td>
<td></td>
</tr>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search Result</td>
<td>Lists sites found and shows the territory, if any, to which each belongs. Select a site and click the right arrow to open the Add Site Link dialog.</td>
</tr>
<tr>
<td>Associated Sites</td>
<td>Lists sites linked to the cloud and shows the territory, if any, to which each belongs.</td>
</tr>
</tbody>
</table>

4. Click OK.

Edit a Network Cloud
You can edit an MPLS network cloud in the RealPresence DMA system's site topology.

Procedure
  1. Go to Service Config > Site Topology > Network Clouds.
  2. Choose a network cloud from the list, and click Edit in the Actions list.
  3. In the Edit Network Cloud dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Info</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the cloud (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the cloud (up to 200 characters).</td>
</tr>
</tbody>
</table>

**Associated Sites**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search Result</td>
<td>Lists sites found and shows the territory, if any, to which each belongs.</td>
</tr>
<tr>
<td></td>
<td>Select a site and click the right arrow to open the Add Site Link dialog.</td>
</tr>
<tr>
<td>Associated Sites</td>
<td>Lists sites linked to the cloud and shows the territory, if any, to which each belongs.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Site Links**

Links between sites must be configured in order to enable calls between sites.

For an endpoint in site A to call an endpoint in site B, there must be a link path connecting site A and site B. A site link can connect two sites, or it can connect a site to an MPLS network cloud.

An initial site link is provided by default, named Default Site to Internet/VPN. It links the default site with the Internet/VPN site to allow call routing for a newly deployed system.

If the system is integrated with a RealPresence Resource Manager system, it receives this information from that system, and you cannot modify any site link information. If the RealPresence DMA system is not integrated with a RealPresence Resource Manager system, you can enter link information.

**Add a Site Link**

You can define a new site link in the RealPresence Resource Manager system’s site topology.

A link can connect two sites, or it can connect a site to an MPLS network cloud.

**Procedure**

1. Go to **Service Config > Site Topology > Site Links**.
2. In the **Actions** list, click **Add**.
3. In the **Add Site Link** dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name for the link (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the link (up to 200 characters).</td>
</tr>
<tr>
<td>From site</td>
<td>The originating site of the link.</td>
</tr>
<tr>
<td>To site</td>
<td>The destination site of the link.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls, which you set at the gateway or router.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls, which you set at the gateway or router. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

4. Click OK.

Related Links
Call Server Settings on page 297

Edit a Site Link

You can edit a site link in the RealPresence Resource Manager system's site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud. You can't change the sites that a site link connects. To modify how sites are linked, delete the links to be removed and add the new links.

Procedure
1. Go to Service Config > Site Topology > Site Links.
2. Choose a site from the list, and click Edit in the Actions list.
3. In the Edit Site Link dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name for the link (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the link (up to 200 characters).</td>
</tr>
<tr>
<td>From site</td>
<td>The originating site of the link (view only).</td>
</tr>
<tr>
<td>To site</td>
<td>The destination site of the link (view only).</td>
</tr>
<tr>
<td>Max total bandwidth (Mbps)</td>
<td>The total bandwidth limit for voice and video calls, which you set at the gateway or router.</td>
</tr>
<tr>
<td>Max per-call bit rate (kbps)</td>
<td>The per-call bit rate limit for voice and video calls, which you set at the gateway or router. When you specify both the bandwidth and bit rate limits, the dialog shows you how many calls at that bit rate the specified bandwidth supports. The value of the Bit rate to bandwidth conversion factor setting on the Call Server Settings page is used in this calculation.</td>
</tr>
</tbody>
</table>

4. Click OK.

Related Links
Call Server Settings on page 297
Site-to-Site Exclusions

The site-to-site exclusions are site-to-site connections that the site topology does not permit a call or session to use.

If the system is integrated with a RealPresence Resource Manager system, it receives this information from that system, and this page is read-only. If not, you can define exclusions.

View Site-to-Site Exclusions

You can view a list of any site-to-site exclusions that exist in your site topology.

Procedure

» Go to Service Config > Site Topology > Site-to-Site Exclusions.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From site</td>
<td>Name of one of the two sites connected by the excluded link.</td>
</tr>
<tr>
<td>To site</td>
<td>Name of the other site.</td>
</tr>
</tbody>
</table>

Add a Site-to-Site Exclusion

You can define a new site-to-site exclusion in the RealPresence DMA system's site topology.

Procedure

1. Go to Service Config > Site Topology > Site-to-Site Exclusions.
2. In the Actions list, click Add.
3. In Step 1 of the wizard, select the first site for the exclusion.
4. Click Next.
5. In Step 2 of the wizard, select the second site for the exclusion.
6. Click Next.
7. In Step 3 of the wizard, review the exclusion and click Done if it's correct.

Territories

A territory contains one or more sites for which a RealPresence DMA cluster is responsible.

By default, there is one territory named Default DMA Territory.

In a superclustered RealPresence DMA system deployment, additional territories allow you to assign different territories to different RealPresence DMA clusters and to specify a backup cluster for each territory to increase fault tolerance. If a territory's primary cluster becomes unavailable for any reason, the backup cluster takes over the responsibilities for the territory.

Territories serve the following purposes:
• Sites are associated with territories, thus specifying which RealPresence DMA cluster is responsible for serving as the H.323 gatekeeper, SIP registrar, and SIP proxy for each site.

• Microsoft Active Directory integration is associated with a territory, thus specifying which RealPresence DMA cluster is responsible for connecting to the directory server, retrieving user and group data, and updating the shared supercluster data.

• Microsoft Exchange server integration (for calendaring service) is associated with a territory, thus specifying which RealPresence DMA cluster is responsible for integrating with the Exchange server and monitoring the Conferencing infrastructure mailbox.

• The RealPresence DMA system’s conference manager functionality is associated with territories, thus specifying which RealPresence DMA clusters are responsible for hosting conference rooms (VMRs). Up to three territories (and thus clusters) may have this responsibility.

If the system is integrated with a RealPresence Resource Manager system, it receives territory information from that system, and the Territories page is view-only. If not, you can modify the territory information.

**View the Territories List**

You can view the list of territories that have been added to your site topology.

**Procedure**

1. Go to **Service Config > Site Topology > Territories**.
2. On the right, it displays information about the selected territory.

   The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column/Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the territory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the territory.</td>
</tr>
<tr>
<td>Primary cluster</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Backup cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory.</td>
</tr>
<tr>
<td></td>
<td>You must have a supercluster consisting of at least two RealPresence</td>
</tr>
<tr>
<td></td>
<td>DMA clusters in order to specify a backup.</td>
</tr>
<tr>
<td>Host conference rooms</td>
<td>Indicates whether this territory is used for hosting conference rooms (VMRs).</td>
</tr>
<tr>
<td>Territory summary pane</td>
<td>Repeats the name and description of the selected territory.</td>
</tr>
<tr>
<td>Associated sites pane</td>
<td>List the sites included in the selected territory.</td>
</tr>
</tbody>
</table>

**Add a Territory**

You can define a new territory in the system’s site topology.

**Procedure**

1. **Navigate to Service Config > Site Topology > Territories.**
2. In the **Actions** list, click **Add**.

3. In the **Add Territory** dialog, edit the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Territory Info</strong></td>
<td>A meaningful name for the territory (up to 128 characters).</td>
</tr>
<tr>
<td>Name</td>
<td>A brief description of the territory (up to 200 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Primary cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory.</td>
</tr>
<tr>
<td>Host conference rooms in this territory</td>
<td>Enables this territory to be used for hosting conference rooms (VMRs).</td>
</tr>
<tr>
<td></td>
<td>The territory's primary and backup clusters must both be enabled for</td>
</tr>
<tr>
<td></td>
<td>conference room hosting. No more than three territories may have this</td>
</tr>
<tr>
<td></td>
<td>capability enabled.</td>
</tr>
<tr>
<td>Associated Sites</td>
<td>Enter search string or leave blank to find all sites.</td>
</tr>
<tr>
<td>Search sites</td>
<td>Lists sites found and shows the territory, if any, to which each currently</td>
</tr>
<tr>
<td></td>
<td>belongs.</td>
</tr>
<tr>
<td>Available sites</td>
<td>Selecting a site and moving it to the <strong>Associated sites</strong> list changes its</td>
</tr>
<tr>
<td></td>
<td>territory assignment to this territory.</td>
</tr>
<tr>
<td>Associated sites</td>
<td>Lists sites linked to this territory. Changes you make to this list aren't</td>
</tr>
<tr>
<td></td>
<td>implemented until you click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

4. Click **OK**.

**Edit a Territory**

You can revise a territory in your system’s site topology as needed.

**Procedure**

1. Go to **Service Config > Site Topology > Territories**.
2. Select the territory to edit.
3. Under **Actions**, click **Edit**.
4. Edit the fields in the following table as needed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Territory Info</strong></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the territory (up to 128 characters).</td>
</tr>
<tr>
<td>Description</td>
<td>A brief description of the territory (up to 200 characters).</td>
</tr>
<tr>
<td>Primary cluster</td>
<td>The primary RealPresence DMA cluster responsible for this territory.</td>
</tr>
<tr>
<td>Backup cluster</td>
<td>The backup RealPresence DMA cluster, if any, responsible for this territory. You must have a supercluster consisting of at least two RealPresence DMA clusters in order to specify a backup.</td>
</tr>
<tr>
<td>Host conference rooms in this territory</td>
<td>Enables this territory to be used for hosting conference rooms (VMRs). The territory's primary and backup clusters must both be enabled for conference room hosting. No more than three territories may have this capability enabled.</td>
</tr>
</tbody>
</table>

**Associated Sites**

<table>
<thead>
<tr>
<th>Search sites</th>
<th>Enter search string or leave blank to find all sites.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available sites</td>
<td>Lists sites found and shows the territory, if any, to which each currently belongs. Selecting a site and moving it to the Associated sites list changes its territory assignment to this territory.</td>
</tr>
<tr>
<td>Associated sites</td>
<td>Lists sites linked to this territory. Changes you make to this list aren't implemented until you click OK.</td>
</tr>
</tbody>
</table>

5. Click OK.
Users and Groups

Topics:

- User Roles and Access Privileges
- Users
- Groups
- Login Policy Settings

This section provides an introduction to managing local and enterprise users and groups in the Polycom RealPresence DMA system.
User Roles and Access Privileges

Topics:

- User Roles
- User Access Privileges

The RealPresence DMA system has four user roles, or classes of users, each with its own set of permissions.

Every user account has one or more user roles, but three of the four roles must be explicitly assigned.

Related Links
Set Up Security

User Roles

If your system is integrated with a Microsoft Active Directory, all enterprise users are automatically assigned the role of Conferencing User.

You can use enterprise groups to manage assignment of the other user roles.

Note: You must be an enterprise user with the appropriate user role assignments to see and work with enterprise users in the RealPresence DMA management user interface. A local user can only see other local users, regardless of user roles.

The following table describes the user roles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>The administrator is responsible for the overall administration of the system and can access all the management user interface pages except those reserved for auditors. You must be an enterprise user to see enterprise reports, enterprise users, and groups. If you have a RealPresence Resource Manager system, assign this role to its login account. If API access for other clients is enabled, assign this role to the login account of any other API client that should have administrative rights and responsibilities. This role must be assigned by an administrator.</td>
</tr>
<tr>
<td>Auditor</td>
<td>The auditor is responsible for configuring logging and history record retention, and for managing logs. An auditor can access all history reports. This role must be assigned by an administrator.</td>
</tr>
</tbody>
</table>
### Role Description

**Provisioner**
A provisioner is responsible for the management of **Conferencing User** accounts.

A provisioner can create or modify users that only have the **Conferencing User** role, but can view all local users. A user with this role can also view history reports.

You must be an enterprise user to view all enterprise users.

If you have a RealPresence Resource Manager system or any other API client, assign this role to its users who should have provisioning rights and responsibilities.

This role must be assigned by an administrator.

**Conferencing user**
A conferencing user is provisioned with a conference room (VMR) or rooms and can host conferences. A conferencing user cannot access the management user interface.

This role is automatically present on all user accounts. It is not listed under **Available Roles** or explicitly assigned.

For API access, the system identifies a subcategory of conferencing user, the conference room owner, who can monitor and control their conferences.

### Related Links
- Integrate with Active Directory on page 201
- Set Up Security
- Active Directory Cache Refresh Frequency on page 207
- Managing Users on page 450
- Generate an Orphaned Groups and Users Report on page 208
- View the Active Directory Page on page 212
- Assign Conference Properties to a Group on page 479
- Edit a User on page 453
- Conference Settings on page 245
- Conference Templates on page 249
- MCU Pools and Pool Orders on page 190

### User Access Privileges

The RealPresence Resource Manager system has three user roles that provide access to the management user interface and the RealPresence Platform application programming interface (API).

Depending on your user role or roles, you can access different parts of the interface and perform different functions, as shown in the following table:

<table>
<thead>
<tr>
<th>Menu/Icon</th>
<th>Admin</th>
<th>Provisioner</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Calls</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoints</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>High Availability Status</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Sessions¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site Statistics¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site Link Statistics¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Network Usage</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>TURN Allocations</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users²</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Login Policy Settings &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local User Account</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Password</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Access Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DMAs</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MCU¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>RealPresence Resource Manager</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polycom ContentConnect</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External SIP Peers¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>External H.323 Gatekeepers¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>External H.323 SBCs¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Microsoft Active Directory²</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Skype Systems</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Tunnel Settings</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>DMA Edge Wizard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Service Config</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Manager Settings &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Templates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU Pools¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MCU Pool Orders¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Shared Number Dialing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IVR Prompt Sets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Conference Factories</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence Publishing for Skype</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Server Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Dial Plan &gt;</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial Plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix Service</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Hunt Groups</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Domain Restrictions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Site Topology &gt;</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sites¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site Links¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Site-to-Site Exclusions¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Network Clouds¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Territories¹</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACL Variables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACL Rules</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>ACL Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Policies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded DNS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Proxy Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TURN Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Traversal Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Port Ranges</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.323 Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebRTC Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reports</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call History</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference History</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration History</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert History</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACL Denials</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS Active Directory Reports &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orphaned Groups and Users</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Admin</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Availability Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Menu/Icon</td>
<td>Admin</td>
<td>Provisioner</td>
<td>Auditor</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>SNMP Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alert Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Configuration Assistant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Linux Root Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Linux Remote Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Log Files^4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History Retention Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Utilities &gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Packet Capture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traceroute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O Stats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Upgrade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup and Restore</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown and Restart</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td>-------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Help Contents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search Documentation Library (Web)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RealPresence Platform API Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>About RealPresence DMA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

^4 System Log Files are accessible to all user roles.
<table>
<thead>
<tr>
<th>Menu/Icon</th>
<th>Admin</th>
<th>Provisioner</th>
<th>Auditor</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶️ - Alerts/messages</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>⏰ - Refresh interval</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>💾 - User role, for example, Admin.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>🤓 - Help. Opens the online help for the page you’re viewing.</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
</tbody>
</table>

1. Provisioners have view-only access.
2. Must be an enterprise user to see enterprise users. Provisioners cannot add or remove roles or endpoints, and cannot edit user accounts with explicitly assigned roles (administrator, provisioner, or auditor), but can manage their conference rooms.
3. Must be an enterprise user to view this report.
4. Administrators cannot delete log archives.
In the RealPresence DMA system, you can manage two types of users: local and enterprise.

**Local** users are added manually to the RealPresence DMA system. When you manually add users, you can assign them conference rooms and specific user roles.

**Enterprise** users are added automatically as RealPresence DMA system users when you integrate your system with a Microsoft Active Directory. This integration allows users with specific roles such as Administrator, Auditor, or Provisioner to log into the RealPresence DMA system with their Active Directory user names and passwords. The integration process can also automatically create conference rooms for enterprise users based on the Active Directory field (such as phone number) that you specify.

Enterprise users are automatically assigned a Conferencing User role and they display in the **Users** list. An administrator can assign additional roles as required.

In addition to managing local and enterprise users, you can assign and manage different types of conference rooms and associate endpoints with specific users.

---

**Note:** You must be an enterprise user with the appropriate user role assignments to view and work with enterprise users in the RealPresence DMA system. A local user can only view other local users, regardless of user roles.

### Managing Users

A newly installed RealPresence DMA system has two local user accounts: `admin` and `rppuser`.

The `rppuser` account is populated with the factory default configuration, has the same default password as `admin`, and is not assigned any user roles. Five VMRs configured with factory default settings are assigned to the `rppuser` account. You can use these VMRs to make test calls on a newly deployed system.

The `admin` account is a user account with Administrator privileges. As part of the initial system setup, Polycom recommends that you create a local user account for yourself with the Administrator role, log in using that account, then delete the `admin` user account. You can then create other local user accounts or integrate with an Active Directory and assign additional roles to the appropriate enterprise users.

If you plan to integrate with a RealPresence Resource Manager system, you must create a local user account for the RealPresence Resource Managersystem, which enables that system to log in to the RealPresence DMA system’s RealPresence Platform API. This account should have Administrator and Provisioner roles.

The RealPresence Resource Manager user owns the VMR conference rooms that the system creates for preset dialout conferences. These are called Anytime conferences in the RealPresence Resource Manager system.
Add a Local User

You can add a local user to the RealPresence DMA system and assign roles to the user.

**Note:** If Cisco Codian MCUs are included in the RealPresence DMA system's pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

**Procedure**

1. Go to **User > Users**.
2. Under the **Actions** list, click **Add**.
3. Complete the fields in the following table as required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>The local user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The local user's last name.</td>
</tr>
<tr>
<td>User ID</td>
<td>The local user's login name.</td>
</tr>
<tr>
<td>Password</td>
<td>The local user's system login password. This is the password that enables users with explicitly assigned roles to log into the system's management interface. This is not the conference or chairperson passcode. The password must satisfy the local password rules specified for the system.</td>
</tr>
<tr>
<td>Email address</td>
<td>The local user's email address.</td>
</tr>
<tr>
<td>User pass-through to CDR</td>
<td>An optional value to put in the <strong>userDataA</strong> field of call detail records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.</td>
</tr>
<tr>
<td>Account disabled</td>
<td>If selected, the user cannot host conferences. The user's conference room or rooms will not be available. In addition, the user will not be able to access the system's management interface. You can select the check box and still create the user account, but not activate it immediately.</td>
</tr>
</tbody>
</table>

**Note:**

- If Cisco Codian MCUs are included in the RealPresence DMA system's pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.
### Field | Description
--- | ---
Conference room territory | The territory to which the user's VMR conference rooms are assigned. A conference room's territory assignment determines which RealPresence DMA cluster hosts the room's conferences. The RealPresence DMA system will use the primary cluster for the territory, or its backup cluster if necessary.

If not selected, the user's conference rooms are assigned in priority order as follows:
- To the territory specifically associated with the room.
- To the territory associated with the Active Directory group that the user belongs to. If the user belongs to more than one Active Directory Group, then the conference rooms are assigned to the territory associated with the group that is alphabetically first.
- To the system's default territory.

Class of service | Select to assign the user a class of service, which determines the priority of the user's calls.

If not selected, the user receives the highest class of service associated with any group to which the user belongs. If the user does not belong to any group, the user will receive the system's default class of service.

A class of service may also be assigned to an endpoint. The class of service of the device applies to point-to-point calls. VMR calls use the conference room's class of service.

Maximum bit rate (kbps) | If **Class of service** is selected, you can specify the maximum bit rate for the user.

### Associated Roles

### Field | Description
--- | ---
Available roles | Lists the roles available to assign to the user. All users are automatically assigned the **Conferencing User** role, but it is not listed or explicitly assigned.

**Note:** Explicitly assigned roles give the user access to the system's management interface.
### Conference Passcodes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson passcode</td>
<td>The numeric passcode that identifies chairpersons in the user's conferences. If you do not identify a chairperson passcode, the user's conferences will not include the chairperson feature. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The chairperson passcode cannot be the same as the conference passcode. The chairperson passcode can also be set individually for each of the user's conference rooms.</td>
</tr>
<tr>
<td>Conference passcode</td>
<td>The numeric passcode that callers must enter to join the user's conferences. If you do not identify a conference passcode, the user's conferences will not require a passcode. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The conference passcode cannot be the same as the chairperson passcode. The conference passcode can also be set individually for each of the user's conference rooms.</td>
</tr>
</tbody>
</table>

4. Click OK.

### Edit a User

You can change all details for a local user except for the user ID.

You can change an enterprise user's roles and their chairperson and conference passcodes. You can also enable or disable their accounts. You cannot change an enterprise user's name, user ID, or user password.

**Note:** If Cisco Codian MCUs are included in the RealPresence DMA system's pool of conferencing resources, do not assign a chairperson passcode without also assigning a conference passcode. If a conference with only one passcode (either chairperson or conference) lands on a Codian MCU, all callers to the conference must enter that passcode.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want, then click **Search**. This will display users that match your criteria.
3. Select the user to edit.
4. Click **Edit** in the **Actions** list.
5. In the **Edit User** window, edit the fields as described in the following table.

#### General Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>The local user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The local user's last name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User ID</td>
<td>The local user's login name.</td>
</tr>
<tr>
<td>Password</td>
<td>The local user's system login password. This is the password that enables users with explicitly assigned roles to log into the system's management interface. This is not the conference or chairperson passcode.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>The password must satisfy the local password rules specified for the system.</td>
</tr>
<tr>
<td>Email address</td>
<td>The local user's email address.</td>
</tr>
<tr>
<td>User pass-through to CDR</td>
<td>An optional value to put in the <strong>userDataA</strong> field of call detail records (CDRs) associated with this user. For example, this might be a user ID from some external system or database.</td>
</tr>
<tr>
<td>Account disabled</td>
<td>If selected, the user cannot host conferences. The user's conference room or rooms will not be available. In addition, the user will not be able to access the system's management interface. You can select the check box and still create the user account, but not activate it immediately.</td>
</tr>
<tr>
<td>Conference room territory</td>
<td>The territory to which the user's VMR conference rooms are assigned.</td>
</tr>
<tr>
<td></td>
<td>A conference room's territory assignment determines which RealPresence DMA cluster hosts the room's conferences. The RealPresence DMA system will use the primary cluster for the territory, or its backup cluster if necessary.</td>
</tr>
<tr>
<td></td>
<td>If not selected, the user's conference rooms are assigned in priority order as follows:</td>
</tr>
<tr>
<td></td>
<td>• To the territory specifically associated with the room.</td>
</tr>
<tr>
<td></td>
<td>• To the territory associated with the Active Directory group that the user belongs to. If the user belongs to more than one Active Directory Group, then the conference rooms are assigned to the territory associated with the group that is alphabetically first.</td>
</tr>
<tr>
<td></td>
<td>• To the system's default territory.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to assign the user a class of service, which determines the priority of the user's calls.</td>
</tr>
<tr>
<td></td>
<td>If not selected, the user receives the highest class of service associated with any group to which the user belongs. If the user does not belong to any group, the user will receive the system's default class of service.</td>
</tr>
<tr>
<td></td>
<td>A class of service may also be assigned to an endpoint. The class of service of the device applies to point-to-point calls. VMR calls use the conference room's class of service.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>If <strong>Class of service</strong> is selected, you can specify the maximum bit rate for the user.</td>
</tr>
</tbody>
</table>
### Associated Roles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available roles</td>
<td>Lists the roles available to assign to the user. All users are automatically assigned the <strong>Conferencing User</strong> role, but it is not listed or explicitly assigned. <strong>Note:</strong> Explicitly assigned roles give the user access to the system's management interface.</td>
</tr>
</tbody>
</table>

---

### Conference Passcodes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson passcode</td>
<td>The numeric passcode that identifies chairpersons in the user's conferences. If you do not identify a chairperson passcode, the user's conferences will not include the chairperson feature. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The chairperson passcode cannot be the same as the conference passcode. The chairperson passcode can also be set individually for each of the user's conference rooms.</td>
</tr>
<tr>
<td>Conference passcode</td>
<td>The numeric passcode that callers must enter to join the user's conferences. If you do not identify a conference passcode, the user's conferences will not require a passcode. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The conference passcode cannot be the same as the chairperson passcode. The conference passcode can also be set individually for each of the user's conference rooms.</td>
</tr>
</tbody>
</table>

---

6. Click **OK**.

**Related Links**
- [Conference Settings](#) on page 245
- [Conference Templates](#) on page 249
- [MCU Pools and Pool Orders](#) on page 190
- [User Roles](#) on page 443

**Find a User**

You can search for specific local or enterprise users based on search strings, search filters, and wildcards (*).

The system matches the exact string you enter against the user ID, first name, and last name. If you enter `sam`, the system displays users with IDs, first, or last names are `sam`, but the results will not include IDs, first, or last names of `samuels`. To search for a user when you have only a partial user ID or name, you can use an asterisk (*) as a wildcard. For example, to find users with the user ID, first, or last name of `samuels`, enter any of the following search strings:

- `sa*`
• sam*ls
• *ls

Procedure
1. Go to User > Users.
2. For a simple search, enter a search string in the Search field and press Enter.
3. For more search options, click the filter button to the right of the Search field.
4. Select the filters you want, enter search strings for one or more fields, then click Search.

The following information displays about the users that match your search criteria:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user's login name. The icon to the left indicates whether the user's account is enabled or disabled. Hover over it to see the associated message.</td>
</tr>
<tr>
<td>First name</td>
<td>The user's first name.</td>
</tr>
<tr>
<td>Last name</td>
<td>The user's last name.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain associated with the user. All users added manually to the system are in the LOCAL domain.</td>
</tr>
</tbody>
</table>
| Class of service  | The class of service assigned to the user, which determines the priority of the user's calls.  
                      | The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room. |
| Conference rooms  | The user's conference room or rooms (VMRs).  
                      | If the system is integrated with an Active Directory, and you specified criteria for conference room ID generation, the enterprise users have a default conference room assigned to them automatically.  
<pre><code>                  | Alternatively or in addition, enterprise users may have custom conference rooms manually assigned to them. Local users must be manually assigned a conference room or rooms. |
</code></pre>
<p>| Roles             | The user's explicitly assigned user roles. All users automatically have the Conferencing User role; it's not listed or explicitly assigned (but a conference room ID is required). |
| Associated endpoints | The endpoints associated with the user, if any.                               |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passcodes</td>
<td>The numeric passcodes specified for this user, if any:</td>
</tr>
<tr>
<td></td>
<td>▪ Chairperson passcode - Passcode that identifies chairpersons in the user's conferences.</td>
</tr>
<tr>
<td></td>
<td>▪ Conference passcode - Passcode that callers must enter to join the user's conferences.</td>
</tr>
</tbody>
</table>

For enterprise users, passcodes (both kinds) generally come from the Active Directory, but you can specify an enterprise user's passcodes locally by editing the user.

For local users, you can add passcodes when you add or edit the users.

Whether you specify passcodes for a user or not, you can add or change passcodes for a specific conference room of the user's.

5. If more than 100 results display, click the pagination buttons to scroll between groups of results.

If your query matches more than 4000 users, the results will not be sorted.

**Delete a Local User**

You can delete local users from the system when necessary.

**Procedure**

1. Go to User > Users.
2. If necessary, filter the Users list to find the user to be deleted.
   - You can only delete local users, not users added from the Active Directory.
3. Select the user to delete.
4. Click Delete.
5. Click Yes to confirm the deletion.

The user is deleted from the RealPresence DMA system.

**Change Your Local User Password**

You can configure the system to expire local user passwords after a certain number of days.

If your password has expired when you try to log into the system, the Change Password dialog prompts you for a new password.

You can change your password at any time.

**Procedure**

1. Click and select Change Password.
2. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user name that you use to log in. Display only.</td>
</tr>
<tr>
<td>Old password</td>
<td>The password that you want to change.</td>
</tr>
</tbody>
</table>
### Conference Rooms

In the RealPresence DMA system, a user may have three types of conference rooms:

- One enterprise conference room (if this is an enterprise user) automatically assigned to the user as part of the Active Directory integration process. You cannot delete this conference room, but you can modify it.
- Custom conference rooms that you manually add.
- Calendared conference rooms created by the Polycom One Touch Dial App when a user schedules a conference in Microsoft Outlook 365. You can modify some of the settings for these conference rooms, but not the ones set in the Outlook meeting invitation.

In addition, if you have a RealPresence Resource Manager system connected to the RealPresence DMA system's RealPresence Platform API, the RealPresence Resource Manager system can create two types of VMR conference rooms in the RealPresence DMA system:

- Scheduled meeting conference rooms that are short-lived, meaning they have a start and end time. These rooms belong to the Conferencing Users who set up the meetings in the RealPresence DMA system's scheduling interface.
- Preset dialout conference rooms (called Anytime conferences in the RealPresence DMA system), which can be used at any time by someone with the chairperson passcode to initiate a dial-out conference to a preset list of participants. These rooms belong to the user account for the RealPresence DMA system.

### View Conference Rooms

You can view a selected user's VMR conference rooms.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user with the conference rooms to view.
4. Click **Manage Conference Rooms**.

The following information displays in the **Conference Rooms** window:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room ID</td>
<td>The unique ID of the room.</td>
</tr>
<tr>
<td>Dial-in #</td>
<td>The number used to dial into the conference room. The number is automatically set to the dialing prefix plus the room ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Room aliases</td>
<td>The aliases of the conference room that can be dialed to join a conference.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences.</td>
</tr>
<tr>
<td></td>
<td>The template assignment can be made at the conference room level, Active Directory group level, or system default level.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order used by the conference room. This determines which MCU hosts a conference.</td>
</tr>
<tr>
<td></td>
<td>The pool order assignment can be made at the conference room level, Active Directory group level, or system default level.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the conference room is assigned.</td>
</tr>
<tr>
<td></td>
<td>A conference room's territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). The assignment can be made at the conference room level, user level, Active Directory group level, or system default level.</td>
</tr>
<tr>
<td>Max participants</td>
<td>The maximum number of callers allowed to join the conference. <strong>Automatic</strong> means the MCU's maximum is used.</td>
</tr>
<tr>
<td>Initial start time</td>
<td>The start time and date of the meeting as provided by the calendaring application.</td>
</tr>
<tr>
<td>Expiration time</td>
<td>The end time and date of the meeting as provided by the calendaring application.</td>
</tr>
</tbody>
</table>

**Related Links**

- [Conference Settings](#) on page 245
- [Conference Templates](#) on page 249
- [MCU Pools and Pool Orders](#) on page 190

**Add a Conference Room for a User**

You can create a custom conference room for any user.

For a local user, you must add at least one conference room to give the user conferencing access.

You can create additional custom conference rooms for a local or enterprise user to offer a different conferencing experience (for example, by assigning a different conference template to the room), or an alternate room ID and dial-in number.

If a room's conference template is linked to a RealPresence Collaboration Server or RMX profile, the profile's IVR service determines whether callers are prompted for passcodes:

- If the profile's IVR service prompts for passcodes, callers are prompted even if the conference doesn't have a passcode.
- If the profile's IVR service doesn't prompt for passcodes, callers aren't prompted even if the conference has a conference or chairperson passcode.
Procedure
1. Go to User > Users.
2. Enter the search criteria, then click Search.
   Users that match your criteria display.
3. Select the user for whom to add a conference room.
4. Click Manage Conference Rooms.
5. In the Conference Rooms window, click Add.
6. In the Add Conference Room window, complete the fields as described in the following table:

### General Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room ID</td>
<td>The unique ID of the conference room. Enter a Room ID or click Generate to let the system pick a random available ID from the range set in Conference Settings. Valid Room IDs must meet the following requirements: • Must start and end with an alphanumeric character. • Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ &amp; , . ' = + - * ( ) % is allowed if it is followed by at least three alphanumeric characters. • Cannot contain blank spaces.</td>
</tr>
<tr>
<td>Dial-in #</td>
<td>The number used to dial into the conference room. Automatically set to the dialing prefix plus the room ID.</td>
</tr>
<tr>
<td>Conference template</td>
<td>The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences. If you don't select the check box, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system's default template. If this template is linked to a RealPresence Collaboration Server or RMX profile, the profile's IVR service determines whether callers are prompted for passcodes: • If the profile's IVR service prompts for passcodes, callers are prompted even if the conference doesn't have a passcode. • If the profile's IVR service doesn't prompt for passcodes, callers aren't prompted even if the conference has a conference or chairperson passcode.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max participants</td>
<td>Select the check box to allow the maximum number of callers to join the conference room. Select the Automatic check box if you want the MCU to use its default maximum.</td>
</tr>
<tr>
<td></td>
<td>To manually set the maximum number of callers that can join the room, select the Max Participants check box, then select the maximum number of callers in the field next to the check box.</td>
</tr>
<tr>
<td></td>
<td>If you don't select the Max Participants check box, the conference room uses the system's default maximum.</td>
</tr>
<tr>
<td>Chairperson required</td>
<td>If you select the check box, the conference will only start when a chairperson joins the conference. The user or conference room should be configured with a chairperson passcode or chairperson alias. This setting applies even if Conference requires chairperson is not selected in the conference template.</td>
</tr>
<tr>
<td>Presence</td>
<td>In a Lync 2013 or Skype for Business 2015 environment, you can configure presence publishing (the publishing of VMR status to a Skype client contact list) for each VMR. When selected, this check box overrides the system-wide default presence publishing settings defined in Presence Publishing for Skype.</td>
</tr>
<tr>
<td></td>
<td>This option is only visible if you select the Publish presence for Polycom conference contacts check box in the Presence Publishing for Skype settings.</td>
</tr>
<tr>
<td></td>
<td>There are two modes of operation for the Presence field, which depend on the check box settings for Publish presence for Polycom conference contacts and Create Polycom conference contacts:</td>
</tr>
<tr>
<td></td>
<td>When Publish presence for Polycom conference contacts is checked and Create Polycom conference contacts is unchecked, the following options display:</td>
</tr>
<tr>
<td></td>
<td>• Publish presence</td>
</tr>
<tr>
<td></td>
<td>• Do not publish presence</td>
</tr>
<tr>
<td></td>
<td>These options control whether the RealPresence DMA system will publish presence status for the Polycom conference contact.</td>
</tr>
<tr>
<td></td>
<td>When both the Publish presence for Polycom conference contacts and Create Polycom conference contacts check boxes are selected, the following options display:</td>
</tr>
<tr>
<td></td>
<td>• Create contact and publish presence</td>
</tr>
<tr>
<td></td>
<td>• Do not create contact or publish presence</td>
</tr>
<tr>
<td></td>
<td>These options control whether the RealPresence DMA system will create an Active Directory contact resource and publish presence for the Polycom conference contact.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Conference duration</td>
<td>Select the check box to configure the maximum duration of a conference in <strong>Hours</strong> and <strong>Minutes</strong>, or <strong>Unlimited</strong>. The maximum duration depends on the MCU.</td>
</tr>
<tr>
<td></td>
<td>If you don't select the check box, the room uses the longest duration associated with any group to which the user belongs. If the user does not belong to any groups, the room will use the system's default maximum duration.</td>
</tr>
<tr>
<td></td>
<td><strong>Duration overrides last disconnect</strong> - If you select this option, an active conference will continue until the conference duration is reached, even if all participants have left the conference. This allows participants to join or rejoin the conference using the passcodes that are current for the conference. This is useful when the conference chairperson has changed the passcodes during the conference or when the conference room passcodes have changed during the conference. If not selected, participants dialing in would use the settings in the conference room. If selected, participants dialing in would use the settings current for the conference.</td>
</tr>
<tr>
<td>Territory</td>
<td>The territory to which the conference room is assigned.</td>
</tr>
<tr>
<td></td>
<td>A conference room's territory assignment determines which RealPresence DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary).</td>
</tr>
<tr>
<td></td>
<td>If you don't select the check box, the conference room is assigned as follows (in priority order listed):</td>
</tr>
<tr>
<td></td>
<td>• To the territory associated with the user.</td>
</tr>
<tr>
<td></td>
<td>• To the territory associated with the Active Directory group the user belongs to (if more than one, the lexically first group).</td>
</tr>
<tr>
<td></td>
<td>• To the system's default territory.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order used by this conference room to determine which MCU hosts a conference.</td>
</tr>
<tr>
<td></td>
<td>If you don't select the check box, the room uses the highest-priority pool order associated with any group to which the user belongs, or if none, the system's default pool order.</td>
</tr>
<tr>
<td>MCU selection</td>
<td>Select the check box to configure the RealPresence DMA system's method of selecting MCUs from MCU pool orders:</td>
</tr>
<tr>
<td></td>
<td>Choose <strong>Prefer MCU in first MCU pool</strong> to ensure that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.</td>
</tr>
<tr>
<td></td>
<td>Choose <strong>Prefer MCU in first caller's site</strong> to match the MCU chosen for the call with the site that the first caller's endpoint belongs to.</td>
</tr>
<tr>
<td>Conference room pass-through to CDR</td>
<td>Optional value to put in the <strong>userDataA</strong> field of conference call detail records (CDRs) associated with this user.</td>
</tr>
<tr>
<td></td>
<td>For example, this might be a user ID from an external system or database.</td>
</tr>
</tbody>
</table>
### Passcodes and Aliases

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chairperson passcode</td>
<td>The numeric passcode that identifies chairpersons in this room's conferences. If none, the room's conferences do not include the chairperson feature.</td>
</tr>
<tr>
<td></td>
<td>If the user has a chairperson passcode, it displays here. You can change it to a different passcode for this room only.</td>
</tr>
<tr>
<td></td>
<td>Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The Chairperson passcode cannot be the same as the conference passcode.</td>
</tr>
<tr>
<td>Use as alias</td>
<td>If you select the check box, the RealPresence DMA system creates a Conference room alias from the Chairperson passcode and assigns the Chairperson role for the alias. The role and alias display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference passcode</td>
<td>The numeric passcode that participants must enter to join the room's conferences. If none, the room's conferences do not require a passcode.</td>
</tr>
<tr>
<td></td>
<td>If the user has a conference passcode, it appears here. You can change it to a different passcode for this room only.</td>
</tr>
<tr>
<td></td>
<td>Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.</td>
</tr>
<tr>
<td>Use as alias</td>
<td>If you select the check box, the RealPresence DMA system creates a Conference room alias from the Conference passcode and assigns Participant as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference room alias</td>
<td>The alias of the conference room that can be dialed to join a conference. Can contain alphanumeric and special characters. Cannot contain spaces.</td>
</tr>
<tr>
<td>Conference role</td>
<td>The specific conference role associated with the conference room alias. If the role assigned to the Conference room alias is then the caller is prompted for a passcode when they dial the conference room alias. If the caller enters the chairperson passcode, they enter the conference as a chairperson.</td>
</tr>
<tr>
<td></td>
<td>If the Chairperson conference role has been assigned to the conference alias, the caller joins the conference as a chairperson, without being prompted for the chairperson passcode.</td>
</tr>
</tbody>
</table>
Preset Dialouts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Preset dialouts            | If you select the **Enabled** check box, this conference room is for a preset dialout conference, referred to in the RealPresence Resource Manager system as an **Anytime** conference. When someone dials in and starts a conference, the RealPresence DMA system dials out to the entries in the **Preset Dialout Participants** list. For the RealPresence DMA system to perform an H.323 dialout from a conference or to establish a cascade link between MCUs, the Polycom RealPresence Collaboration Server (MCU) hosting the conference must be H.323-registered to one of the RealPresence DMA clusters in the supercluster. The system does not forward dialouts to endpoints with call forwarding activated. Disabling **Preset Dialouts** lets you turn off the automatic dialout temporarily without losing the configuration data. To prevent unauthorized persons from being able to trigger the dialout, do the following:  
  ▪ Set **Conference template** to a template that requires a chairperson to start the conference.  
  ▪ Specify a chairperson passcode for this conference room or this user. If the conference template in use requires a chairperson, the dialout does not occur until the first chairperson has joined, regardless of the number of other participants in the conference. Similarly, if the conference includes a conference passcode, the dialout will not occur until a participant enters the passcode successfully. |
| Preset dialout participants | Lists the names and URIs of the participants that the RealPresence DMA system automatically dials when the conference starts. If an icon appears in the **Settings** column for a participant, hover your mouse cursor over the icon for more information.                                                                                                                                                                                                                                  |

Scheduling and Integration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial start time</td>
<td>The start time of a single conference or the start time for the first meeting in a recurring series.</td>
</tr>
<tr>
<td>Expiration time</td>
<td>The end time of a single conference or the end time for the last meeting in a recurring series.</td>
</tr>
<tr>
<td>Conference focus URI</td>
<td>The sip URI that identifies the Skype for Business conference to which this VMR will be connected. As part of the Polycom RealConnect solution for Microsoft Office 365, the PolycomOne Touch Dial App will populate this value from Office 365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.</td>
</tr>
</tbody>
</table>
### Field Description

**Destination network**
The host name, FQDN, or network domain label, with or without port and URL parameters, of the Microsoft federated environment (Lync, Skype for Business, or Office 365) that is hosting the conference.

This field is required when the Microsoft environment is federated and the focus URI does not provide a correct destination network. You can leave the field blank if the Microsoft environment is not federated.

**Note:** For Microsoft Office 365 conferences, the Polycom One Touch Dial App will populate this value from Office 365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.

### AS-SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource priority namespace</td>
<td>In an assured services SIP (AS-SIP) environment, a local session controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. If your organization has implemented such a resource prioritization mechanism and you want to assign this conference room a priority value different from the system's default, set this field to the namespace being used for resource priority values. If the namespace being used is not listed, select <strong>Custom</strong> and enter the name in the box below the list.</td>
</tr>
<tr>
<td>Resource priority value</td>
<td>If the RealPresence DMA system is deployed in an AS-SIP environment with a resource prioritization mechanism and LSC, set this to the priority value to assign to conferences using this conference room. If using a custom namespace, enter the value in the box below the list. The string <code>namespace:value</code> is used in the <strong>SIP Resource-Priority</strong> header of outbound calls from this conference room and recorded in the conference property changes.</td>
</tr>
</tbody>
</table>

7. Click **OK**.

**Related Links**
- [Conference Settings](#) on page 245
- [Conference Templates](#) on page 249
- [MCU Pools and Pool Orders](#) on page 190

**Edit a Conference Room for a User**

You can revise a conference room's details as needed.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user with the conference room to edit.
4. Click **Manage Conference Rooms**.
5. In the **Conference Rooms** window, select a conference room from the list and click **Edit**.
6. In the **Edit Conference Room** window, revise the fields described in the following table as needed:

**General Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Room ID            | The unique ID of the conference room. Enter a **Room ID** or click **Generate** to let the system pick a random available ID from the range set in **Conference Settings**. Valid Room IDs must meet the following requirements:  
  - Must start and end with an alphanumeric character.  
  - Characters in the middle may be alphanumeric or any of the following: _ ~ ! $ & , . ' = + - * ( )  
  - % is allowed if it is followed by at least three alphanumeric characters.  
  - Cannot contain blank spaces. |
| Dial-in #          | The number used to dial into the conference room. Automatically set to the dialing prefix plus the room ID.                                      |
| Conference template| The template used by the conference room, which defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences.  
  If you don't select the check box, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system's default template.  
  If this template is linked to a RealPresence Collaboration Server or RMX profile, the profile's IVR service determines whether callers are prompted for passcodes:  
  - If the profile's IVR service prompts for passcodes, callers are prompted even if the conference doesn't have a passcode.  
  - If the profile's IVR service doesn't prompt for passcodes, callers aren't prompted even if the conference has a conference or chairperson passcode. |
| Max participants   | Select the check box to allow the maximum number of callers to join the conference room. Select the **Automatic** check box if you want the MCU to use its default maximum.  
  To manually set the maximum number of callers that can join the room, select the **Max Participants** check box, then select the maximum number of callers in the field next to the check box.  
  If you don't select the **Max Participants** check box, the conference room uses the system's default maximum. |
| Chairperson required| If you select the check box, the conference will only start when a chairperson joins the conference. The user or conference room should be configured with a chairperson passcode or chairperson alias. This setting applies even if **Conference requires chairperson** is not selected in the conference template. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Presence                          | In a Lync 2013 or Skype for Business 2015 environment, you can configure presence publishing (the publishing of VMR status to a Skype client contact list) for each VMR. When selected, this check box overrides the system-wide default presence publishing settings defined in **Presence Publishing for Skype**.

This option is only visible if you select the **Publish presence for Polycom conference contacts** check box in the **Presence Publishing for Skype** settings.

There are two modes of operation for the **Presence** field, which depend on the check box settings for **Publish presence for Polycom conference contacts** and **Create Polycom conference contacts**:

When **Publish presence for Polycom conference contacts** is checked and **Create Polycom conference contacts** is unchecked, the following options display:

- Publish presence
- Do not publish presence

These options control whether the RealPresence DMA system will publish presence status for the Polycom conference contact.

When both the **Publish presence for Polycom conference contacts** and **Create Polycom conference contacts** check boxes are selected, the following options display:

- Create contact and publish presence
- Do not create contact or publish presence

These options control whether the RealPresence DMA system will create an Active Directory contact resource and publish presence for the Polycom conference contact.

| Conference duration               | Select the check box to configure the maximum duration of a conference in **Hours** and **Minutes**, or **Unlimited**. The maximum duration depends on the MCU.

If you don't select the check box, the room uses the longest duration associated with any group to which the user belongs. If the user does not belong to any groups, the room will use the system's default maximum duration.

**Duration overrides last disconnect** - If you select this option, an active conference will continue until the conference duration is reached, even if all participants have left the conference. This allows participants to join or rejoin the conference using the passcodes that are current for the conference. This is useful when the conference chairperson has changed the passcodes during the conference or when the conference room passcodes have changed during the conference. If not selected, participants dialing in would use the settings in the conference room. If selected, participants dialing in would use the settings current for the conference. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territory</td>
<td>The territory to which the conference room is assigned. A conference room’s territory assignment determines which RealPresence DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary). If you don’t select the check box, the conference room is assigned as follows (in priority order listed): ▪ To the territory associated with the user. ▪ To the territory associated with the Active Directory group the user belongs to (if more than one, the lexically first group). ▪ To the system’s default territory.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>The MCU pool order used by this conference room to determine which MCU hosts a conference. If you don’t select the check box, the room uses the highest-priority pool order associated with any group to which the user belongs, or if none, the system’s default pool order.</td>
</tr>
</tbody>
</table>
| MCU selection              | Select the check box to configure the RealPresence DMA system’s method of selecting MCUs from MCU pool orders:  
  Choose **Prefer MCU in first MCU pool** to ensure that the DMA system always routes the call to the first available MCU in the first MCU pool. If no MCU is available, the system searches the second MCU pool for an available MCU, and so on.  
  Choose **Prefer MCU in first caller’s site** to match the MCU chosen for the call with the site that the first caller’s endpoint belongs to. |
| Conference room pass-through to CDR | Optional value to put in the **userDataA** field of conference call detail records (CDRs) associated with this user.  
For example, this might be a user ID from an external system or database. |

### Passcodes and Aliases

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Chairperson passcode   | The numeric passcode that identifies chairpersons in this room’s conferences. If none, the room’s conferences do not include the chairperson feature.  
If the user has a chairperson passcode, it displays here. You can change it to a different passcode for this room only.  
Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. The Chairperson passcode cannot be the same as the conference passcode. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use as alias</td>
<td>If you select the check box, the RealPresence DMA system creates a Conference room alias from the Chairperson passcode and assigns the Chairperson role for the alias. The role and alias display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference passcode</td>
<td>The numeric passcode that participants must enter to join the room's conferences. If none, the room's conferences do not require a passcode. If the user has a conference passcode, it appears here. You can change it to a different passcode for this room only. Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Cannot be the same as the chairperson passcode.</td>
</tr>
<tr>
<td>Use as alias</td>
<td>If you select the check box, the RealPresence DMA system creates a Conference room alias from the Conference passcode and assigns Participant as the role for the alias. The alias and role display in the Conference Room Alias and Conference Role list.</td>
</tr>
<tr>
<td>Conference room alias</td>
<td>The alias of the conference room that can be dialed to join a conference. Can contain alphanumeric and special characters. Cannot contain spaces.</td>
</tr>
<tr>
<td>Conference role</td>
<td>The specific conference role associated with the conference room alias. If the role assigned to the Conference room alias is then the caller is prompted for a passcode when they dial the conference room alias. If the caller enters the chairperson passcode, they enter the conference as a chairperson. If the Chairperson conference role has been assigned to the conference alias, the caller joins the conference as a chairperson, without being prompted for the chairperson passcode.</td>
</tr>
</tbody>
</table>
### Preset Dialouts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preset dialouts</td>
<td>If you select the <strong>Enabled</strong> check box, this conference room is for a preset dialout conference, referred to in the RealPresence Resource Manager system as an <strong>Anytime</strong> conference. When someone dials in and starts a conference, the RealPresence DMA system dials out to the entries in the <strong>Preset Dialout Participants</strong> list.</td>
</tr>
<tr>
<td></td>
<td>For the RealPresence DMA system to perform an H.323 dialout from a conference or to establish a cascade link between MCUs, the Polycom RealPresence Collaboration Server (MCU) hosting the conference must be H.323-registered to one of the RealPresence DMA clusters in the supercluster.</td>
</tr>
<tr>
<td></td>
<td>The system does not forward dialouts to endpoints with call forwarding activated.</td>
</tr>
<tr>
<td></td>
<td>Disabling <strong>Preset Dialouts</strong> lets you turn off the automatic dialout temporarily without losing the configuration data.</td>
</tr>
<tr>
<td></td>
<td>To prevent unauthorized persons from being able to trigger the dialout, do the following:</td>
</tr>
<tr>
<td></td>
<td>▪ Set <strong>Conference template</strong> to a template that requires a chairperson to start the conference.</td>
</tr>
<tr>
<td></td>
<td>▪ Specify a chairperson passcode for this conference room or this user.</td>
</tr>
<tr>
<td></td>
<td>If the conference template in use requires a chairperson, the dialout does not occur until the first chairperson has joined, regardless of the number of other participants in the conference. Similarly, if the conference includes a conference passcode, the dialout will not occur until a participant enters the passcode successfully.</td>
</tr>
<tr>
<td>Preset dialout participants</td>
<td>Lists the names and URIs of the participants that the RealPresence DMA system automatically dials when the conference starts.</td>
</tr>
<tr>
<td></td>
<td>If an icon appears in the <strong>Settings</strong> column for a participant, hover your mouse cursor over the icon for more information.</td>
</tr>
</tbody>
</table>

### Scheduling and Integration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial start time</td>
<td>The start time of a single conference or the start time for the first meeting in a recurring series.</td>
</tr>
<tr>
<td>Expiration time</td>
<td>The end time of a single conference or the end time for the last meeting in a recurring series.</td>
</tr>
<tr>
<td>Conference focus URI</td>
<td>The sip URI that identifies the Skype for Business conference to which this VMR will be connected. As part of the Polycom RealConnect solution for Microsoft Office 365, the PolycomOne Touch Dial App will populate this value from Office 365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.</td>
</tr>
</tbody>
</table>
### Destination network

The host name, FQDN, or network domain label, with or without port and URL parameters, of the Microsoft federated environment (Lync, Skype for Business, or Office 365) that is hosting the conference.

This field is required when the Microsoft environment is federated and the focus URI does not provide a correct destination network. You can leave the field blank if the Microsoft environment is not federated.

**Note:** For Microsoft Office 365 conferences, the Polycom One Touch Dial App will populate this value from Office 365 calendared meetings. For other Skype for Business deployments, this value may be obtained from the Skype system.

### AS-SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource priority namespace</td>
<td>In an assured services SIP (AS-SIP) environment, a local session controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. If your organization has implemented such a resource prioritization mechanism and you want to assign this conference room a priority value different from the system’s default, set this field to the namespace being used for resource priority values. If the namespace being used is not listed, select <strong>Custom</strong> and enter the name in the box below the list.</td>
</tr>
<tr>
<td>Resource priority value</td>
<td>If the RealPresence DMA system is deployed in an AS-SIP environment with a resource prioritization mechanism and LSC, set this to the priority value to assign to conferences using this conference room. If using a custom namespace, enter the value in the box below the list. The string <code>namespace:value</code> is used in the <strong>SIP Resource-Priority</strong> header of outbound calls from this conference room and recorded in the conference property changes.</td>
</tr>
</tbody>
</table>

7. Click OK.

**Related Links**
- Working with MCU Pool Orders on page 194
- Conference Settings on page 245
- Conference Templates on page 249
- MCU Pools and Pool Orders on page 190

### Delete a Conference Room for a User

You can delete custom conference rooms for a user that you added manually in the RealPresence DMA system or via the API.

You cannot delete enterprise conference rooms, calendared meeting conference rooms (Polycom Conferencing for Outlook), or scheduled conference rooms created by the Polycom RealPresence Resource Manager system via the API.

**Procedure**

1. Go to **User > Users**.
2. Select the user with the custom conference room you want to delete.
3. Click Manage Conference Rooms.
4. In the Conference Rooms window, select the conference room to delete and click Delete.
5. Click Yes to delete the selected conference room.

Add a Conference Room Alias and Conference Role
An alias is an alternative way to dial to join a conference.
When a caller dials in to a conference using an alias, they join the conference with the conference role associated with that alias. For example, if the conference alias has been assigned the Chairperson conference role, the caller joins the conference as a Chairperson, without being prompted for the Chairperson passcode.

Procedure
1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user for whom to add the conference room alias and conference role.
4. Click Manage Conference Rooms.
5. Select an existing conference room from the list and click Edit, or Add a new one.
6. In the Add Conference Room or Edit Conference Room window, select the Passcodes and Aliases section.
7. Click Add.
8. In the Add Conference Room Alias window, do one of the following:
   a. Click Generate to automatically create an alias for the conference room.
   b. Enter an alias of your own choosing.
9. Under Conference Role, select the role to associate with the conference room alias.
10. Click OK.

Edit a Conference Room Alias and Conference Role
In the RealPresence DMA system, you can edit or generate a new alias for a conference room and change the conference role associated with an alias.

Note that it is not required to change both a conference room alias and its conference role.

Procedure
1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user with the conference room alias or conference role to edit.
4. Click Manage Conference Rooms.
5. Select an existing conference room from the list and click Edit.
6. In the Edit Conference Room window, select the Passcodes and Aliases section.
7. Select a Conference Room Alias and click Edit.
8. In the Edit Conference Room Alias window, click Generate or enter a new value if you want to create a new alias for the conference room.
9. Under **Conference Role**, choose a new role to associate with the conference room alias, if desired.
10. Click **OK**.

## Delete a Conference Room Alias and Conference Role

You can delete a conference room alias and its associated role from the RealPresence DMA system as needed.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to delete.
4. Click **Manage Conference Rooms**.
5. Select an existing conference room from the list and click **Edit**.
6. In the **Edit Conference Room** window, select the **Passcodes and Aliases** section.
7. Select a **Conference Room Alias** and click **Delete**.
8. Click **Yes** to confirm the deletion.

## Add a Dialout Participant

You can add a conference participant to a conference room's **Preset Dialout Participants** list.

When someone dials into the conference room and starts a conference, the RealPresence DMA system dials out to the participants in the list.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to add to the **Preset Dialout Participants** list.
4. Click **Manage Conference Rooms**.
5. Select an existing conference room from the list and click **Edit**, or add a new one.
6. In the **Add Conference Room** or **Edit Conference Room** window, select **Preset Dialouts**.
7. Select the **Enabled** check box.
8. Click **Add**.
9. In the **Add Dialout Participant** window, complete the fields as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant name</td>
<td>The name of the participant.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used to dial the participant (SIP, H.323, ISDN).</td>
</tr>
<tr>
<td>Dial-out URI</td>
<td>Dial string used to dial the participant. If you select SIP or ISDN as the Protocol, the system adds a schema (for example, sip: or isdn:) before the URI.</td>
</tr>
<tr>
<td>Extension</td>
<td>You can specify optional extension digits for ISDN dial-out connections. The characters # and p are allowed.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Connection encryption | Available for H.323 and ISDN connections only. If enabled or if you select **Yes**, the system instructs the MCU to encrypt this participant's connection.

Line rate | Select **Automatic** or select the specific **Rate (kbps)** to use for dial-out calls to the participant.

Audio-only | Available for H.323 and ISDN connections only. If enabled, the system instructs the MCU to use an audio-only connection for this participant.

Auto disconnect | Available for H.323 and ISDN connections only. Any dial-out participants you mark as Auto-disconnect are automatically disconnected once they are the only participants left in the conference. After they are disconnected, the conference ends. You can use this feature to prevent MCU-to-MCU dial-outs from remaining open after the conference has ended.

10. Click **OK**.

### Edit a Dialout Participant

You can edit a participant in a conference room's **Preset Dialout Participants** list, changing the name or dial string for the participant.

The RealPresence DMA system dials out to the participants in the list.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to edit.
4. Click **Manage Conference Rooms**.
5. Select an existing conference room from the list and click **Edit**.
6. In the **Edit Conference Room** window, select the **Preset Dialouts** section.
7. Ensure the **Enabled** check box is checked.
8. Select a dial-out participant from the list.
9. Click **Edit**.
10. In the **Edit Dialout Participant** window, edit the following fields as required:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant name</td>
<td>The name of the participant.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol used to dial the participant (SIP, H.323, ISDN).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dial-out URI</td>
<td>Dial string used to dial the participant. If you select SIP or ISDN as the Protocol, the system adds a schema (for example, sip: or isdn:) before the URI.</td>
</tr>
<tr>
<td>Extension</td>
<td>You can specify optional extension digits for ISDN dial-out connections. The characters # and p are allowed.</td>
</tr>
<tr>
<td>Connection encryption</td>
<td>Available for H.323 and ISDN connections only. If enabled or if you select Yes, the system instructs the MCU to encrypt this participant's connection.</td>
</tr>
<tr>
<td>Line rate</td>
<td>Select Automatic or select the specific Rate (kbps) to use for dial-out calls to the participant.</td>
</tr>
<tr>
<td>Audio-only</td>
<td>Available for H.323 and ISDN connections only. If enabled, the system instructs the MCU to use an audio-only connection for this participant.</td>
</tr>
<tr>
<td>Auto disconnect</td>
<td>Available for H.323 and ISDN connections only. Any dial-out participants you mark as Auto-disconnect are automatically disconnected once they are the only participants left in the conference. After they are disconnected, the conference ends. You can use this feature to prevent MCU-to-MCU dial-outs from remaining open after the conference has ended.</td>
</tr>
</tbody>
</table>

11. Click OK.

Delete a Dial-out Participant

You can delete a participant in a conference room's Preset Dialout Participants list when necessary.

Procedure

1. Go to User > Users.
2. Enter the search criteria you want and click Search to display users that match your criteria.
3. Select the user to delete.
4. Click Manage Conf Rooms.
5. Select an existing conference room from the list and click Edit.
6. In the Edit Conference Room window, select the Preset Dialouts section.
7. Ensure the Enabled check box is checked.
8. Select the dial-out participant to delete from the list.
9. Click Delete.

Associated Endpoints

Users can be associated with or disassociated from specific endpoints.

You can also manage user-to-device associations on the Endpoints page.
Associate a User with a Device

You can associate a user with an endpoint by selecting the user, then searching for the endpoint to associate with the user.

You can search by device **Alias, IP Address, Name, Model, Owner, Owner domain** or, a combination of these criteria.

The system matches the search string you enter against the beginning of the field you are searching. For example, if you enter `sa` in the endpoint **Name** field, the search results display endpoints with names that begin with `sa`. To search for a matching string not at the beginning of the field, you can use an asterisk (`*`) as a wildcard, such as `*sa`.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to associate with an endpoint.
4. Click **Manage Associated Endpoints**.
   - The **Associated Endpoints** window displays the endpoints associated with the user, if any.
5. Click **Add**.
6. In the **Select Associated Endpoints** window, search for endpoints based on the criteria you enter.
7. Select one or more endpoints to associate with the user.
   - Use **Shift-click** or **Ctrl-click** to select multiple endpoints.
8. Click **OK**, then click **OK** again.

Disassociate a User from a Device

You can disassociate a user from an endpoint by selecting the user, then deleting the association.

Note that deleting the association does not delete the endpoint.

**Procedure**

1. Go to **User > Users**.
2. Enter the search criteria you want and click **Search** to display users that match your criteria.
3. Select the user to disassociate from an endpoint.
4. Click **Manage Associated Endpoints**.
   - The **Associated Endpoints** window displays the endpoints associated with the user.
5. Select one or more endpoints to disassociate and click **Delete**.
6. Click **Yes** to confirm the disassociation.
Groups

Topics:

- View Groups
- Working with Enterprise Groups

If you've integrated your RealPresence DMA system with a Microsoft Active Directory, you can assign roles and conference templates associated with user groups after you've imported the groups you want to use.

Groups functionality is available only if your RealPresence DMA system is integrated with an Active Directory. User groups are defined in your Active Directory and imported into the RealPresence DMA system.

You must be an enterprise user (with the appropriate user role assignments) to see and work with enterprise users. A local user can only see other local users, regardless of user roles.

Microsoft Active Directory provides two group types and four group scopes. The RealPresence DMA system supports only security groups (not distribution groups) with universal or global scope.

View Groups

The Groups page provides information about enterprise groups.

Procedure

- Go to User > Groups.

The following table describes the fields on the Groups page:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Name of the group, as defined in the Active Directory.</td>
</tr>
<tr>
<td>Description</td>
<td>Description from the Active Directory.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain to which the group belongs.</td>
</tr>
</tbody>
</table>
| Class of service  | Class of service assigned to the group, which determines the priority of the group's calls.  
If none, the group receives the system's default class of service defined in Conference Settings.  
A class of service may also be assigned to a user or an endpoint.  
The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room. |
**Working with Enterprise Groups**

You can customize the conferencing experience for members of an Active Directory group by assigning it a conference template.

In addition, you can set RealPresence DMA user roles on a group basis, which allows you to manage RealPresence DMA administrative access according to groups.

You must be logged in to the RealPresence DMA system as an enterprise user with the Administrator role to perform these procedures.

**Import Enterprise Groups**

After you’ve integrated your RealPresence DMA system with Active Directory, you can import enterprise groups to the RealPresence DMA system.

**Procedure**

1. Go to **User > Groups**.
2. Click **Import Enterprise Groups**.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search domain</td>
<td>Optionally, select a domain to search.</td>
</tr>
</tbody>
</table>

---

**Table:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference template</td>
<td>Template assigned to the group that defines the conference properties (or links to the Polycom MCU conference profile) used for the group's conferences. You can assign a template at the conference room, AD group, or system default level.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>MCU pool order assigned to this group that is used to determine which MCU hosts a conference. You can assign the pool order assignment at the conference room, AD group, or system default level.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the group's conference rooms (VMRs) are assigned. A conference room's territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). You can assign a territory at the conference room level, the user level, the AD group level, or the system default level.</td>
</tr>
<tr>
<td>Assigned roles</td>
<td>RealPresence DMA system roles, if any, that are automatically assigned to members of this group (all users automatically have the Conferencing User role; it's not listed or explicitly assigned).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>To find all groups, leave blank. To find groups beginning with a specific letter or letters, enter the string. Then click <strong>Search</strong>. You can use a wildcard (*) for more complex searches, such as:</td>
</tr>
</tbody>
</table>
|               |   • s*admins  
|               |   • *eng*                                                                                                                                         |
| **Search results** | Lists the security groups in your Active Directory that match the search string.  
The system only retrieves the first 1000 groups found. If the count shows 1000, you may need to refine your search criteria. |
| **Groups to import** | Lists the groups you've selected for import, using the arrows to move them from the **Search results** box.                                                                 |

4. Click **OK**.

### Set Up an Enterprise Group

Because the **RealPresence DMA** system does not allow you to add or edit groups you import from Active Directory, you must create any custom groups you may need within your Active Directory system and then import them.

For example, you can configure an enterprise group for users who need access to the system's management user interface. After importing the group to your RealPresence DMA system, you can assign the group a specific role.

**Procedure**

1. In your Active Directory, create a security group containing the users to whom you want to give access to the RealPresence DMA system's management user interface.  
   You can assign all the user roles to a single group or create separate groups for each user role.
2. In the RealPresence DMA system, go to **User > Groups**.
3. Click **Import Enterprise Groups**.
4. Use **Search** to find the security group you created.
5. Move the group to the **Groups to import** box and click **OK**.
6. On the **Groups** page, select your new group.
7. Click **Edit**.
8. Move the user roles you want to give members of this group to the **Selected roles** box.
9. Click **OK**.  
   All members of this group will now share the system access privileges you assigned to the group.
10. To grant RealPresence DMA system access privileges to a user or remove those privileges, add or remove the user from the appropriate enterprise group.

### Assign Conference Properties to a Group

You can assign the group a class of service, a template, an MCU pool, and more.
Procedure
1. Go to User > Groups.
2. Select the group of interest and click Edit.
3. Complete the following fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service</td>
<td>Select to assign the group a class of service other than the system's default. The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>If Class of service is selected, specifies the maximum bit rate for the group.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>If Class of service is selected, specifies the minimum bit rate to which the group's calls can be reduced (downspeeded).</td>
</tr>
<tr>
<td>Conference template</td>
<td>Select to assign a template other than the system's default. The template assignment can be made at the conference room level, AD group level, or system default level. It defines the conference properties (or links to the Polycom MCU conference profile) used for its conferences.</td>
</tr>
<tr>
<td>MCU pool order</td>
<td>Select to assign the group an MCU pool order other than the system's default. The pool order assignment can be made at the conference room level, AD group level, or system default level. It's used to determine which MCU hosts a conference.</td>
</tr>
<tr>
<td>Territory</td>
<td>Select to assign the group's conference rooms to a territory other than the system's default. A conference room's territory assignment determines which RealPresence DMA cluster hosts the conference (the primary cluster for the territory, or its backup cluster if necessary). The assignment can be made at the conference room level, user level, AD group level, or system default level. If a user belongs to more than one group, that user's territory setting is inherited from the lexically first group (but does not change if the group is renamed). To be certain that a specific user's conference rooms are assigned to a specific territory, assign that territory directly to the user.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Presence publishing options | In a Microsoft Lync 2013 environment, you can configure presence publishing (the publishing of VMR status to a Lync 2013 client contact list) for any VMR that belongs to a member of this group. Enable this check box to override the system-wide default presence publishing settings defined on the Conference Settings page.

This property is visible only if the Publish presence for Polycom conference contacts check box is enabled on the Conference Settings page.

This property can be overridden on a per-VMR basis by the Presence setting on the User > Users > Manage Conference Rooms dialog.

Depending on the settings of the Publish presence for Polycom conference contacts and Create Polycom conference contacts check boxes on the Conference Settings page, there are two modes of operation for this field:

- When Publish presence for Polycom conference contacts is checked and Create Polycom conference contacts is unchecked, the following options are displayed:
  - Publish presence
  - Do not publish presence

  These options control whether the RealPresence DMA system will publish presence status for VMRs belonging to members of this group.

- When both Publish presence for Polycom conference contacts and Create Polycom conference contacts are checked, the following options are displayed:
  - Create contact and publish presence
  - Do not create contact or publish presence

  These options control whether the RealPresence DMA system will create an Active Directory contact resource for and publish presence for VMRs that belong to members of this group.

Default conference duration | Select to specify a maximum conference duration other than the system's default. If you select Unlimited, the maximum depends on the MCU.

Available roles | Lists the RealPresence DMA system roles available for automatic assignment to members of this group (all users automatically have the Conferencing User role; it's not listed or explicitly assigned).

Use the arrows to move roles from the Available roles box to the Selected roles box or vice versa.

Selected roles | Lists the roles you've selected for members of this group.

Remember, ordinary Conferencing Users have no explicitly assigned role.

4. Click OK.

**Related Links**

[Conference Settings](#) on page 245
Assign an MCU Pool Order to a Group
You can specify which MCUs a group uses by assigning an MCU pool order to the group.

Procedure
1. If necessary, create the MCU pool and the pool order needed.
2. Go to User > Groups.
3. Select the group to which to assign the pool order.
4. Click Edit.
5. In the MCU pool order list, select the pool order to be used for this group.
6. Click OK.

Assign a Conference Template to a Group
You can set up a custom conferencing experience for an enterprise group by assigning a conference template to that group.

Procedure
1. Go to Service Config > Conference Manager Settings > Conference Templates and create a template that defines the conferencing experience for this group.
2. Optionally, under Actions, click Move Up until your new conference template has Priority 1. This ensures that users who have access to multiple conference templates will use this one for their enterprise conference room. You can choose a different priority level, but then some members of the group for which you created the template may use a higher-ranking template.
3. Go to User > Groups.
4. Select the group for which you created the template.
5. Click Edit.
6. Select the template you created for this group.
7. Click OK.
Login Policy Settings

Topics:

- Configure Local User Account Settings
- Configure Local Password Settings
- Configure Session Settings
- Configure Banner Settings
- Management Access Settings

Login Policy Settings enable you to configure some security aspects of user access to the RealPresence DMA system.

Related Links
Set Up Security

Configure Local User Account Settings

From the Local User Account page, you can perform the following actions:

- Lock out users who have exceeded the specified number and frequency of login failures. The system locks the account either indefinitely or for the length of time you specify.
- Disable accounts that have been inactive a specified number of days.

Procedure

1. Go to User > Login Policy Settings > Local User Account.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Account Lockout</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable account lockout</td>
<td>Turns on lockout feature and enables lockout configuration fields below.</td>
</tr>
<tr>
<td>Failed login threshold</td>
<td>Specify how many consecutive login failures cause the system to lock an account.</td>
</tr>
<tr>
<td>Failed login window (hours)</td>
<td>Specify the time span within which the consecutive failures must occur in order to lock the account.</td>
</tr>
<tr>
<td>Customize user account lockout duration (minutes)</td>
<td>If selected, specify how long the user's account remains locked. If not selected, the lockout is indefinite, and a user with a locked account must contact an Administrator to unlock it.</td>
</tr>
</tbody>
</table>
Account Inactivity

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize account inactivity threshold (days)</td>
<td>Turns on disabling of inactive accounts and lets you specify the inactivity threshold that triggers disabling.</td>
</tr>
</tbody>
</table>

3. Click **Update** to save your settings.

Configure Local Password Settings

From the **Local Password** page, you can specify age, length, and complexity requirements for the passwords of local administrator, auditor, and provisioner users.

These rules don’t apply to conferencing user’s conference and chairperson passcodes, or to Active Directory users.

**Procedure**

1. Go to **User > Login Policy Settings > Local Password**.
2. Complete the fields in the following table as needed:

**Password Management**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum password age (days)</td>
<td>The age at which a password expires (30-180 days).</td>
</tr>
<tr>
<td>Minimum password age (days)</td>
<td>Specifies how frequently a password can be changed (1-30 days).</td>
</tr>
<tr>
<td>Minimum length</td>
<td>The number of characters a password must contain (1-30).</td>
</tr>
<tr>
<td>Minimum changed characters</td>
<td>The number of characters that must be different from the previous password (1-4).</td>
</tr>
<tr>
<td>Reject previous passwords</td>
<td>Specifies how many of the user’s previous passwords the system remembers and cannot be reused (8-16).</td>
</tr>
</tbody>
</table>

**Password Complexity**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user name or its reverse form</td>
<td>Turns off the protection against a password containing the user's login name or its reverse.</td>
</tr>
<tr>
<td>Lowercase letters</td>
<td>The number of lowercase letters (a-z) that a password must contain.</td>
</tr>
<tr>
<td>Uppercase letters</td>
<td>The number of uppercase letters (A-Z) that a password must contain.</td>
</tr>
<tr>
<td>Numbers</td>
<td>The number of digit characters (0-9) that a password must contain.</td>
</tr>
<tr>
<td>Special characters</td>
<td>The number of non-alphanumeric keyboard characters that a password must contain.</td>
</tr>
</tbody>
</table>
### Configure Session Settings

The RealPresence DMA system enables you to specify the number of simultaneous login sessions by all users and per user ID.

You can also configure the length of login sessions.

Note that in a supercluster, the number of used login sessions is the sum of used sessions for all systems that are part of the supercluster.

Similarly, when High Availability is configured, the number of used login sessions is the sum of all used sessions on both systems in the HA pair.

If you plan on having superclustered systems or HA paired systems, you need to ensure that you have an adequate number of user login sessions to accommodate simultaneous logins on multiple systems.

**Procedure**

1. Go to **User > Login Policy Settings > Session**.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active system sessions</td>
<td>Specify the number of simultaneous login sessions by all users or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to log in is granted access, and the system terminates the non-Administrator session that has been idle the longest.</td>
</tr>
<tr>
<td>Active sessions per user</td>
<td>Specify the number of simultaneous login sessions per user ID or select <strong>Unlimited</strong>.</td>
</tr>
<tr>
<td>Session hard timeout</td>
<td>Specify the length of time after which the system will terminate a session due to lack of activity.</td>
</tr>
</tbody>
</table>

3. Click **Update** to save your settings.

**Related Links**

[Changing the Linux Root Password](#) on page 75

[Login Sessions](#) on page 535
Configure Banner Settings

A login banner is a message that appears when users attempt to access the system. They must acknowledge the message before they can log in.

From the Banner page, you can provide a system description, enable the banner, and select or create the message the banner displays. The message may contain up to 1500 characters.

Procedure

1. Go to User > Login Policy Settings > Banner.
2. Complete the fields in the following table as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System description</td>
<td>Enter a description for the system, for example, Core Configuration or Edge Configuration. The system description displays on the login page and in the menu bar of the management user interface.</td>
</tr>
<tr>
<td>Enable login banner</td>
<td>Enables the display of a login banner. If this box is unchecked, the Message field is disabled. The existing contents, if any, remain unchanged, but aren't displayed to users.</td>
</tr>
<tr>
<td>Message</td>
<td>Select one of the messages from the list, or select Custom and type or paste your own message into the field below. If you select one of the built-in samples, it is copied into the Message field, and you can then edit the copy. When you do so, the system resets the list to Custom. Your edits don't affect the stored sample. You can revert to the original version of the sample by re-selecting it from the list.</td>
</tr>
</tbody>
</table>

3. Click Update to save your settings.

Management Access Settings

The Management Access Settings enable you to restrict access to the management user interface, APIs (port 8443), and SNMP (by default, port 161) to a whitelist of authorized IP addresses or address ranges.

If enabled, the whitelist restrictions take effect as soon as you update the settings. If you enable the whitelist and click Update while logged in from an IP address that is not included in the whitelist, the system warns you that you will not be able to access the system and asks you to confirm the update.

The whitelist settings apply to all clusters in a supercluster. When you join a cluster to a supercluster, the cluster's settings are replaced by those from the supercluster.

Related Links

Set Up Security
Configure Management Access Settings

You can add IP addresses and IP address ranges to an authorized whitelist and delete entries from the whitelist when necessary.

The RealPresence DMA system will accept management connections from the IP addresses and address ranges on ports 8443 (management user interface/API) and 161 (SNMP). Port 8443 can't be changed but you can use a different SNMP port if necessary.

Procedure

1. Go to **User > Login Policy Settings > Management Access Settings**.
2. Select **Enable management access settings**.
   - Enables the input field for IP addresses and restricts management access to the IP addresses or address ranges added to the list.
3. **Add** or **Delete** an IP address or IP address range as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(input field)</td>
<td>Enter an IP address or address range and click <strong>Add</strong> to add it to the list. Enter a range as starting and ending IP addresses, separated by a dash. For example:</td>
</tr>
<tr>
<td></td>
<td><em>(IPv4)</em> 10.33.33.0 - 10.33.34.255</td>
</tr>
<tr>
<td></td>
<td><em>(IPv6)</em> ::1:ffe - ::2:1</td>
</tr>
<tr>
<td>(list)</td>
<td>Select an entry and click <strong>Delete</strong> to remove it from the list.</td>
</tr>
</tbody>
</table>

4. Click **Update** to save your settings.
Maintenance

Topics:

- System Management and Maintenance
- System Log Files
- Backing Up and Restoring
- Upgrading
- Shutting Down and Restarting

This section provides an introduction to Polycom RealPresence DMA system maintenance.
System Management and Maintenance

Topics:

- Administrator Responsibilities
- Recommended Regular Maintenance

The RealPresence DMA system requires some ongoing maintenance beyond monitoring the status of the system and downloading backups and other data you want to archive.

All system management and maintenance tasks can be performed in the management interface.

Administrator Responsibilities

As a RealPresence DMA system administrator, you are responsible for the installation and ongoing maintenance of the system.

You should be familiar with the following configurations, tasks, and operations:

- Installing licenses when the system is first installed and when additional call capacity is added.
- Monitoring system health and performing the recommended regular maintenance.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. Should the need arise, Polycom Global Services personnel may ask you to run these tools.
- Upgrading the system when upgrades/patches are made available.

Administrator Best Practices

The following are some of our recommendations for administrative best practices:

- Perform the recommended regular maintenance.
- Except in emergencies or when instructed to by Polycom Global Services personnel, don't reconfigure, install an upgrade, or restore a backup when there are active calls and conferences on the system. Many of these operations will require a system restart to complete, which will result in these calls and conferences being dropped. Before performing these operations, busy out all MCUs and wait for all conferencing activity to cease.
- Before you reconfigure, install an upgrade, or restore a backup, you should manually create a new backup. Then download and archive this backup in the event that something unforeseen occurs and it becomes necessary to restore the system to a known good state.
- For proper name resolution and smooth network operations, configure two or more DNS servers in your network configuration. This allows the RealPresence DMA system to function properly in the event of a single external DNS failure.
- Configure at least one NTP server in your time configuration and preferably three. Proper time management helps ensure that your cluster operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data.
Auditor Responsibilities

As a RealPresence DMA system auditor, you're responsible for managing the system's logging and history retention.

You should be familiar with the following configurations and operations:

- Configuring logging for the system. These settings affect the number and the contents of the log archives available for download from the system. Polycom Global Services personnel may ask you to adjust the logging configuration and/or download and send them logs.
- Configuring history retention levels for the system. These settings affect how much system activity history is retained on the system and available for download as call data records (CDRs).

Auditor Best Practices

The following are some of our recommendations for auditing best practices:

- Unless otherwise instructed by Polycom Global Services, configure logging at the debug level with a rolling frequency of daily and a retention period of 60 days. If hard drive space becomes an issue, decrease the retention period incrementally until the disk space issue is resolved.
- Download log archives regularly and back them up securely (preferably off-site as well as onsite). Delete downloaded log archives to free up disk space.
- Export CDRs regularly and back them up securely (preferably off-site as well as onsite).

Provisioner Responsibilities

As a RealPresence DMA system provisioner, you have access to many of the same features and functions as the system administrator.

Your responsibilities depend on your organization's policies and the tasks delegated to you by the system administrator. For instance, you may be delegated responsibility for some of the following:

- Managing and monitoring user's conference rooms.
- Managing and monitoring registered endpoints.
- Monitoring active calls.
- Monitoring system health and network usage.
- Monitoring call, conference, and registration history.
- Downloading network usage data at the appropriate intervals.
- Downloading detailed call and conference history data at the appropriate intervals.

Recommended Regular Maintenance

Perform maintenance tasks at least weekly to keep your RealPresence DMA system operating at peak efficiency.

Archive Backups

You should archive backups of your RealPresence DMA system regularly.

Every night, each RealPresence DMA system cluster determines whether its configuration or local user data has changed. If so, it creates a configuration-only backup of the system.
Procedure

1. Log into the RealPresence DMA system.
2. Go to Admin > Backup and Restore and check for new backups.
   If there are new backups, download and archive the latest one. Delete other backups after downloading the latest one in order to free up disk space.

Related Links
Backing Up and Restoring on page 496

Release Resources

You can release the resources of both the locally owned HA node and the peer node, or only the peer node.

Procedure

1. From the High Availability Status page, select Release Resources.
2. Select the virtual IP addresses to release:
   - Both peer and locally-owned VIPs; if you only want to release your own VIPs (for example, if there was no failover, select this option)
   - Only peer-owned VIPs
3. Select Force release now if you want to immediately release resources.
   Selecting this option will terminate all active calls.
4. Click OK.

Check Microsoft Active Directory Health

If your RealPresence DMA system is integrated with a Microsoft Active Directory, you can check the health of the Active Directory system.

Procedure

1. Go to Reports > MS Active Directory Reports.
2. Check the status and results of the last cache update, and verify that membership information for imported groups, if any, was successfully loaded.
3. Go to Reports > Conference Room Errors.
   Check:
   - The total number of users and the number of users with conference room IDs. Make sure both are about what you would expect for your system (it may be helpful to keep records for comparison over time). Contact your Active Directory administrator if necessary.
   - The number of users with blank, invalid, or duplicate conference room IDs. These are enterprise users not properly provisioned for conferencing on the RealPresence DMA system. They’re listed below. Contact your Active Directory administrator to resolve issues with these users.
4. Go to Reports > MS Active Directory Reports > Orphaned Groups and Users and verify that the number of orphans is not unexpectedly large.
5. Go to Reports > Enterprise Passcode Errors.
   If you’re assigning conference and/or chairperson passcodes to enterprise users, verify that the number of passcode errors is not unexpectedly large.
Check Security Configuration
You should regularly check your RealPresence DMA system’s security configuration.

Procedure
» Go to Admin > Server > Security Settings and verify that the security settings are what you expect.
   Any departure from the settings you expect to see may indicate that your system has been compromised.

Check Certificates
You should regularly check the certificates installed on your RealPresence DMA system.

Procedure
1. Go to Admin > Server > Certificates and verify that the list of certificates contains the certificates you have installed (an archived screen capture may be helpful for comparison).
2. Display the details for each certificate you have installed and verify they are accurate (again, an archived screen capture may be helpful for comparison).

Check Network Usage Data Export
You can check your network usage data export.

The RealPresence DMA system stores up to approximately 1 GB of network usage data, deleting the oldest as needed. Data size is based on-site topology complexity, not usage. On a system with the largest supported site topology, it’s only one day’s worth of usage data, but most systems should retain data for a substantially longer period.

Procedure
» Determine an appropriate download interval for your site topology and download network usage data to your local computer during that interval.
System Log Files

Topics:

- Working with System Logs

The System Log Files page lists the available system log file archives.

You can perform the following actions with logs:

- **Roll Logs** - Closes and archives the current log files and starts new log files. If you have a supercluster, you are prompted to choose the cluster whose log files you want to roll.

- **Download Active Logs** - Creates and downloads an archive that contains snapshots of the current log files, but doesn’t close the current log files. If your system is a two-server cluster, you can select which server's logs to download in the File Download dialog.

- **Download Individual Logs** - Downloads the selected individual log file.

- **Download Archived Logs** - Downloads the selected log file archive.

- **Delete Archived Logs** - Deletes the selected log file archive. Only users with the Auditor role can delete archives, and only archives that are downloaded can be deleted. We recommend regularly deleting downloaded log file archives to free up disk space. (The space allocated for log files depends on the size of the system’s local disk.)

- **Show Download History** - Displays the Download History list for the selected log file archive, showing who downloaded the archive and when. This command is only available if the selected archive has been downloaded.

You can change the logging level, rolling frequency, and retention period in Logging Settings.

The archives are Gzip-compressed tar files. Each archive contains a number of individual log files.

The detailed technical data in the log files can help Polycom Global Services resolve problems and provide technical support for your system. Your support representative may ask you to download log archives and send them to Polycom Global Services. You may be asked to manually roll logs so that you can begin gathering new data. After a certain amount of activity, you can download the active logs and send them to Polycom Global Services.

The following table describes the fields in the System Log Files list:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time that the log file archive was created.</td>
</tr>
<tr>
<td>Host</td>
<td>Host name of the server. When the logs are rolled in a two-server cluster (either automatically or manually), an archive is created for each server.</td>
</tr>
<tr>
<td>Filename</td>
<td>Name of the log file archive.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the file in megabytes.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether this is an automatic archive, manual archive, or system snapshot archive (created when you download the active logs).</td>
</tr>
</tbody>
</table>

The following table describes the fields in the Download History list:
### Working with System Logs

You can manually roll logs, download active, individual, and archived logs, and delete archived logs as needed.

#### Manually Roll the System Logs

Manually rolling the system logs closes and archives the current log files and starts new log files. If you have a supercluster, you're prompted to choose the cluster with the log files you want to roll.

**Procedure**

1. Go to Admin > System Log Files.
2. Click **Roll Logs**.
   - If you have a supercluster, you're prompted to choose the cluster with the log files you want to roll.
3. If applicable, select a cluster.
   - Wait a few seconds.
   - The system closes and archives the current log files and starts writing new ones. A dialog informs you that logs have been rolled, and the new log archive appears in the **System Log Files** list. For a two-server cluster, an archive is created for each server.
4. Click **OK**.

#### Download Active Logs

When you download an active log, the RealPresence DMA system creates and downloads an archive that contains snapshots of the current log files, but doesn't close the current log files.

If you have a two-system cluster, you can select which system's logs to download.

**Procedure**

1. Go to Admin > System Log Files.
2. Click **Download Active Logs**.
3. If you have a two-server cluster, in the **Server Name** field, select the server with the logs you want to download.

   4. Click **Download**.
5. Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

---

### Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user ID of the person who downloaded the archive.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time that the archive was downloaded.</td>
</tr>
</tbody>
</table>
Download an Individual Log File

You can select and then download individual active log files.

Procedure

1. Go to Admin > System Log Files.
2. Click Download Individual Logs.
   
   The Download Individual Logs window displays.
3. Select a log file to download and click Download.
4. Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

Download Archived Logs

If you need to examine log files or send them to Polycom support, you can download log archives to your PC.

Procedure

1. Go to Admin > System Log Files.
2. Select the file you want to download from the list of log archives.
3. Click Download Archived Logs.
4. Depending on your browser, specify a location and file name and then save the file, or check your Downloads folder.

Delete a System Log Archive

You can delete system log archives to free disk space.

Note that only users with the Auditor role can delete archives, and only archives that have been downloaded can be deleted.

Procedure

1. Go to Admin > System Log Files.
2. View the Latest Download column to determine if the log archive you want to delete has been downloaded at least once and can be deleted.
3. Select the log archive to delete and verify that the Show Download History command displays.
4. Click Show Download History (optional) to display the Download History list under the list of log archives.
5. Click Delete Archived Logs.
6. Click Yes to confirm the deletion.
Backing Up and Restoring

Topics:

- Backing Up Your System
- Restoring Your System

Polycom recommends that you back up your RealPresence DMA system regularly.

You can create a system backup either on the local server or transfer backup files to a remote server. Local backups are performed and stored independently of remote backups.

In addition to the backups that you create, each RealPresence DMA system cluster automatically creates a locally stored configuration-only backup each night. These configuration-only backups include:

- Local user account information (including local data for enterprise users, such as conference room attributes)
- System configuration data
- Supercluster and resource management system integration data (if applicable)

The backup file is for the cluster, but on a two-server cluster, a copy of the backup exists on each server. This ensures that the backup files are available even if one of the servers isn’t running.

If you want to create a backup that also includes all the transactional data, including logs, CDRs, network usage, and audit (history) data, you should create these manually or schedule backups to be sent to a remote server on your network. The cluster keeps the most recent 10 backups (deleting the oldest backup file when a new one is created).

If you have a superclustered system, you should create backups from each cluster (each cluster’s backup files include only the call, conference, and registration history for that cluster) or transfer the backup files to remote storage.

In most cases, the software version of the backup file must match the system’s current software version to restore from it. Specific releases may include the ability to restore a backup file from earlier versions. Check the release notes for your software version for more information.

The option to omit the IP network configuration makes it possible to clone an existing RealPresence DMA cluster’s feature and system configuration to a new cluster without introducing IP address conflicts.

**Note:** A backup created from a RealPresence DMA edge-configured system can only be restored on an edge system, not on a core-configured system. Likewise, a backup created from a RealPresence DMA core-configured system can only be restored on a core system, not on an edge-configured system.

**Related Links**

- [Archive Backups](#) on page 490
Backing Up Your System

You can create and download backup files of the RealPresence DMA system, then upload the files and use them to restore the system.

You should create and download backups from systems that are part of a supercluster or a High Availability pair.

It's recommended that you download backup files regularly. The system can locally store up to 10 backup files at one time. Delete backup files after downloading to free up disk space on the local system.

Related Links
Set Up Security

View Locally Stored Backup Files

You can store up to 10 backup files on the system concurrently and view the stored backup files as needed.

Procedure

» Go to Admin > Backup and Restore.

The following table describes the fields in the Backup and Restore list. The list contains the last 10 backup files.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation date</td>
<td>Timestamp of the backup file.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the backup file.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the backup file.</td>
</tr>
<tr>
<td>System version</td>
<td>Version number of the application that created the backup file.</td>
</tr>
<tr>
<td>SHA1</td>
<td>SHA1 checksum for the backup file. You can use this to confirm that a downloaded file is an exact copy of one on the server.</td>
</tr>
</tbody>
</table>

Create a New Backup File

You can create a configuration-only backup file or a full backup file.

A full backup adds all transactional data, including logs, CDRs, network usage, and audit (history) data.

The backup file is for the cluster, but on a two-server cluster, a copy of the backup exists on each server. This ensures that the backup files are available even if one of the servers is not running.

The cluster stores the most recent 10 backups, deleting the oldest backup file when a new one is created (unless there are fewer than 10).

Procedure

1. Go to Admin > Backup and Restore.
2. Verify that the oldest backup file listed is one you do not want to keep or have already downloaded.
3. Under Actions, click **Create New (Full)** to create a full backup or **Create New (Config Only)** to create a configuration-only backup (no transaction data).
   
   A confirmation dialog tells you the backup archive was created. For a full backup, this may take some time.

4. Click **OK**.

### Download a Backup File

You can download a backup file to your local computer.

**Procedure**

1. Go to **Admin > Backup and Restore**.
   
   The list contains the last 10 backup files.

2. Select the backup file you want to download.

3. Under Actions, click **Download Selected**.

4. Choose a path and file name for the backup file and click **Save**.
   
   The **File Download** dialog indicates when the download is complete.

5. Click **Close**.

### Upload a Backup File

You can upload a backup file to the RealPresence DMA system for an immediate restore or in preparation for a future manual system restore from the backup file.

Restoring feature and system configuration but not network configuration (or vice versa) will result in invalid primary or backup cluster assignments for some territories. After the restore operation is complete, assign primary and backup clusters to the affected territories.

**Procedure**

1. Go to **Admin > Backup and Restore**.

2. Verify that the oldest backup file listed is one you do not want to keep or have already downloaded.

3. Under Actions, click **Upload**.

4. Choose a backup file to upload and click **Open**.
   
   The system indicates when the upload is complete.

5. Click **Close**.
   
   The system asks if you want to restore now from the backup file you just uploaded.

6. If you do not want to restore (and restart the system) now, click **Manually Later**.

7. To restore now, click **Now**.
   
   The **Confirm Restore** dialog appears.

8. Read the confirmation warning, select which data you want to restore, and click **OK**.
   
   After a short delay, the system will be restored and you will be logged out.

9. Click **OK**.
   
   The system logs you out and the server reboots (typically, this takes about five minutes). After it restarts, in a two-server cluster, the second server syncs to the server that just rebooted so the second server is restored to the same state as the first server. Depending on the configuration changes being applied, the second server may reboot so the changes can take effect.
When done, the LCDs of both the servers display **DMA Clustered** (Polycom Rack Server 630 or 620 systems only).

10. Log back in as a local Administrator user and:
   a. In a two-server cluster, verify on the Dashboard that both servers are up and the private network connection is operating properly.
   b. Go to **Admin > Software Upgrade** and check the **Operation History** table.
   c. If the system was integrated with Active Directory, go to **Integrations > Microsoft Active Directory** and re-enable the integration.

**Configure Remote Backup Settings**

You can schedule system backups for the cluster to run at certain times and use remote file storage. You can configure the date, start time, and frequency of remote backups, as well as remote storage server details. Scheduling remote backups allows you to more easily archive and retain system backups for use in disaster recovery, if needed.

Remote backups are not stored locally; if the system is unable to store the backup archive on the remote storage server, the scheduled backup fails.

**Procedure**

1. Go to the **Admin > Server > Backup Settings** page.
2. Select **Enable automatic backups of this cluster to a remote server (Remote backups will not be retained locally)**.
3. Complete the required fields described in the following table:

| Schedule | 
| --- | --- |
| Remote backup status | Indicates if the system has ever been backed up. |
| Last successful remote backup | The read-only date and time of the last successful scheduled backup. |
| Next remote backup date | A calendar picker allows you to select the date for the next remote backup. |
| Remote backup start time | The time of day that the backup should begin. **Note:** As a best practice, schedule system backups during hours of light system load. This will avoid possible backup-related performance issues during peak hours. |
| Frequency of remote backups (in days) | The number of days between backups at this scheduled time. If you choose 1, the scheduled backup will occur every day. The default value is 7. |
### Backup type

The type of backup the system should perform:
- **Config only** - A backup containing system settings only (no transaction data).
- **Full** - A complete system backup (configuration and transaction data).

The default is Full.

### Remote server

<table>
<thead>
<tr>
<th>Transfer protocol</th>
<th>Choose one of the following protocols when transferring files to the remote storage server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FTP</td>
<td></td>
</tr>
<tr>
<td>• HTTP</td>
<td></td>
</tr>
<tr>
<td>• HTTPS</td>
<td></td>
</tr>
<tr>
<td>• SFTP</td>
<td></td>
</tr>
</tbody>
</table>

The default is SFTP.

<table>
<thead>
<tr>
<th>Hostname or IP address of remote server</th>
<th>The hostname or IP address of the remote storage server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote port</td>
<td>The port the system should use when connecting to the remote server.</td>
</tr>
<tr>
<td>Username</td>
<td>The username the system should use when logging in to the remote storage server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password the system should use when logging in to the remote storage server.</td>
</tr>
<tr>
<td>Remote directory</td>
<td>The directory in which the system should store the backup archive on the remote storage server.</td>
</tr>
<tr>
<td></td>
<td>The directory path must be less than 1000 characters in length and use the forward slash directory delimiter.</td>
</tr>
</tbody>
</table>

4. **Test the settings by clicking Test Settings.**
   The system creates an empty archive and attempts to transfer it to the remote backup server using the configured settings. If successful, a dialog appears confirming the success. If the test fails, a dialog appears stating the reason for the failure.

5. Click **Update** to save the settings or click **Backup Now** to initiate an immediate remote backup.

### Restoring Your System

You can restore system data from a backup file that is stored on the RealPresence DMA system (a single system or one system in an HA pair) or from a backup file stored on a USB flash drive.

Restore from a backup only when there is no activity on the system. Restoring terminates all conferences and reboots the system.
You cannot restore a RealPresence DMA system while it is part of a supercluster. You must manually leave the supercluster first. If the system is responsible for any territories (as primary or backup), you must reassign those territories after restoring the system.

For two systems configured as a HA pair, you need to restore only one system but both systems must be running and communicating.

Note that if you are restoring a backup and the system was integrated with a Polycom RealPresence Resource Manager system when the backup you are restoring was made, that integration is restored. If the system was not integrated when the backup was made, it will no longer be integrated after restoring.

Both types of restore require you to re-integrate with Active Directory after the restore is complete.

**Note:** A backup created from a RealPresence DMA edge-configured system can only be restored on an edge system, not on a core-configured system. Likewise, a backup created from a RealPresence DMA core-configured system can only be restored on a core system, not on an edge-configured system.

---

**Restore from a Backup File on the Cluster**

You can restore system data from a backup file that is stored on the cluster.

Before doing so, make sure that both servers are running and clustered and that there are no running conferences on the system. You should also make sure that all MCUs are out of service.

If you’re restoring a cluster that is part of a supercluster, you must first remove the cluster from the supercluster.

Restoring feature and system configuration but not network configuration (or vice versa) will result in invalid primary or backup cluster assignments for some territories. After the restore operation is complete, assign primary and backup clusters to the affected territories.

If you’ve integrated your system with Active Directory, you’ll need to redo the integration after restoring from a backup file.

**Procedure**

1. Go to **Admin > Backup and Restore**.
2. Select the backup file from which you want to restore.
3. Under **Actions**, click **Restore Selected**.
   
   If the backup file you selected is from a different version of the software, the system displays a warning of the possible consequences if you restore.
4. Confirm that you want to continue.
5. Select the data you want to restore.
   
   The data you can restore depends on:
   - The type of backup file (full or config-only) you selected.
   - For a restore from a non-identical software version, which restore operations the current version supports for the source version data. The options may include:
     - IP network configuration
     - Feature and system configuration
     - History, network usage, and log data
6. Click **OK**.
7. After a short delay, a message informs you that the system will be restored and you will be logged out.

8. Click OK.

The system logs you out and reboots (typically, this takes about 5 minutes). After the system restarts, in a two-server cluster, the second server syncs to it, restoring it to the same state. Depending on the changes being applied, it may reboot so the changes can take effect.

When done, the LCDs of both display DMA Clustered (Polycom Rack Server 630 (R630) or 620 (R620)-based systems only).

9. Log back in as a local admin user and verify the restore:
   a. In a two-server cluster, verify on the Dashboard that both servers are up and the private network connection is operating properly.
   b. Go to Admin > Software Upgrade and check the Operation History table.
   c. If the system was integrated with Active Directory, go to Integrations > Microsoft Active Directory and re-enable the integration.

## Restore from a Backup File on the RealPresence DMA System's USB Flash Drive

If the system is shut down or in a bad state, you can use the Network Configuration Utility to restore the RealPresence DMA system from a backup file (full or configuration-only) that you load onto the USB flash drive.

When you use the Network Configuration Utility to restore a backup, you cannot select which data to restore. If you copy a config-only backup file to the USB flash drive, both the feature and system configuration data and the IP network configuration data will be restored. If you copy a full backup file to the USB flash drive, the transactional (historical) data will also be restored.

If you use the Network Configuration Utility to restore a system while it is part of a supercluster, it's automatically removed from the supercluster.

Only backups from identical versions of the software can be restored using the Network Configuration Utility from a USB flash drive.

### Procedure

1. If the system is running and accessible, log in as an administrator.
2. Make sure that there are no calls on the system and that all MCUs are out of service.
3. Go to Admin > Shutdown and Restart and Shut Down the system.
4. Connect a USB flash drive containing the RealPresence DMA Network Configuration Utility to a client system.
5. Do one of the following to launch the Network Configuration Utility:
   - From a client system running Microsoft Windows, run the `dma7000-usb-gui.exe` file.
   - From a client system running a Unix-based OS (including Mac), run the `runUsbGui.sh` file.
6. In the DMA Network Configuration Utility window, click Copy a Backup to the USB Stick.
7. Select the local backup file from which to restore the system and click Open.
   The utility displays an error message if the file isn't a valid RealPresence DMA system backup. Otherwise, it confirms that the backup file is in place.
9. On a RealPresence DMA server that is powered off, insert the USB flash drive into a USB port.

The server boots and the data in the backup file is applied. Depending on the configuration changes being applied, the server may reboot so the changes can take effect.

11. If this is a two-server cluster:

   a. For a Polycom Rack Server 640 (R640), 630 (R630), or 620 (R620)-based cluster: After the first server has rebooted and its front-panel LCD displays DMA Ready, turn on the second server.

      The second server boots and synchronizes to the first server.

      When done, the LCDs for both the servers display DMA Clustered.

   b. For a Polycom Rack Server 230 (R230) or 220 (R220)-based cluster: After the first server has rebooted and is running, turn on the second server.

      The second server boots and synchronizes to the first server.

12. Log back in as an administrator user and verify the restore:

   a. In a two-server cluster, verify on the Dashboard that both servers are up and the private network connection is operating properly.

   b. Go to Admin > Software Upgrade and check the Operation History table.

   c. If the system was integrated with Active Directory, go to Integrations > Microsoft Active Directory and re-enable the integration.
Upgrading

Topics:

- Disable SIP ALG, H.323 ALG, and Packet Modification on the Network Firewall
- Upgrading the RealPresence DMA System
- Upgrading the RealPresence Access Director System
- Adjust Ports After Upgrading
- Roll Back an Upgrade
- View Upgrade Information

You can upgrade previous versions of the RealPresence DMA system and version 4.2.x of the RealPresence Access Director system.

Before you upgrade either system, review the release notes for the upgrade version.

Upgrading the RealPresence DMA system takes approximately 30-60 minutes but may take longer.

If you upgrade a RealPresence DMA system from version 9.0.x to 10.0.x and a RealPresence Access Director system from version 4.2.x to 10.0.x at the same time, Poly recommends the following:

- First, upgrade your RealPresence DMA system. The 10.0.x system will automatically have a core configuration.
- Next, upgrade your RealPresence Access Director system. The 10.0.x system will automatically have an edge configuration.

Disable SIP ALG, H.323 ALG, and Packet Modification on the Network Firewall

When you install or upgrade the RealPresence DMA system, you need to disable SIP and H.323 ALG and any packet modification on your network firewall.

Call scenarios fail on the RealPresence DMA system if SIP ALG, H.323 ALG, and packet modification are enabled on your network firewall or router. To disable these settings, contact your network firewall administrator.

Note: You can disable the settings before or after you install or upgrade the system.

The following options describe how to determine if your network firewall or router modifies incoming packets.

Procedure

» Do one of the following:
  - Run a sniffer trace and observe the signaling packets (H.323 or SIP) to determine if the network firewall or router inserts its IP address.
  - In the system web interface, go to Monitoring > Endpoints to check if the IP address of the endpoint is the network firewall or router IP address.
Upgrading the RealPresence DMA System

You can upgrade a RealPresence DMA system from the system web interface.

Poly recommends that you upgrade during a maintenance window when there are no active calls or conferences on the system.

**Note:** During an upgrade or rollback, you may need to refresh (or restart) your browser or clear your browser’s cache before you log back into the RealPresence DMA system web interface. This helps to ensure that all system information you view is accurate and current.

Upgrade a RealPresence DMA System

You can upload a software upgrade package and install the upgrade on your system.

Download a recent backup file or take a snapshot of your Virtual Edition instance.

**Note:** Once you start the upgrade process, don’t reboot the server.

**Procedure**

1. Log into Polycom Support.
2. Go to **Documents and Software**.
3. In the **Product/Category** list, select **UC Infrastructure**.
4. Select **Management & Scheduling > RealPresence Distributed Media Application (DMA)**.
5. In the **Current Releases** tab, select the upgrade package to download.
6. Read and accept the End-User License Agreement and the Export Restrictions.
7. Save the upgrade package to your local client system.
8. From the RealPresence DMA system web interface, go to **Admin > Software Upgrade**.
9. Select **Upload and Upgrade**.
10. Go to the upgrade package you saved and select **Open**.
    After the package uploads, the upgrade begins.
11. Select **Upgrade status page** below the status bar.
    The **RPP Install Status** page displays. After the installation status reaches 100 percent, the system reboots.
12. After the system reboots, log in with your administrator credentials.
13. Read and accept the End User License Agreement.
    The system web interface opens.
14. If upgrade alerts display, resolve them to complete the upgrade.

Upgrade High Availability Systems

When you configure two RealPresence DMA systems for High Availability (HA), each of the HA nodes acts as an individual server that you need to upgrade independently.

In both active-passive and active-active RealPresence DMA HA configurations (version 9.0 and later), you can upgrade one node while the other node continues to process calls.
Procedure

1. Before you upgrade the first node, release its resources to the second node.
2. Upgrade the first node.
3. Release the resources of the second node to the first node.
4. Upgrade the second node.

Upgrading RealPresence DMA Systems Integrated with RealPresence Resource Manager

If you integrate your RealPresence DMA system with a RealPresence Resource Manager system, you need to edit the RealPresence DMA instance in the RealPresence Resource Manager system web interface before or after you upgrade.

Edit the RealPresence DMA Instance in the RealPresence Resource Manager System Before You Upgrade

You can edit a RealPresence DMA instance in the RealPresence Resource Manager system before you upgrade.

Revisions won’t interrupt calls and conferences.

Procedure

1. In the RealPresence Resource Manager system web interface, edit the RealPresence DMA instance as follows:
   - Uncheck the Call Server option.
   - Uncheck the Support DMA Supercluster option (if your RealPresence DMA system is part of a supercluster).
2. Upgrade the RealPresence DMA system.
3. In the RealPresence Resource Manager system web interface, edit the RealPresence DMA instance again as follows:
   - Select the Call Server option.
   - Select the Support DMA Supercluster option (if your RealPresence DMA system is part of a supercluster).

Edit the RealPresence DMA Instance in the RealPresence Resource Manager System After You Upgrade

You can edit a RealPresence DMA instance in the RealPresence Resource Manager system after you upgrade.

Revisions won’t interrupt calls and conferences.

Procedure

1. In the RealPresence Resource Manager system web interface, edit the RealPresence DMA instance as follows:
   - Uncheck the Call Server option.
   - Uncheck the Support DMA Supercluster option (if your RealPresence DMA system is part of a supercluster).
2. Edit the RealPresence DMA instance again as follows:
   - Select the Call Server option.
Select the Support DMA Supercluster option (if your RealPresence DMA system is part of a supercluster).

Upgrade a RealPresence DMA System That Has Custom Prompt Sets

If you’ve uploaded custom prompt sets to your RealPresence DMA system, you need to manually change the system backup and restore script before upgrading.

Changing the `sys-backup-restore` script before upgrading enables the custom prompt files to restore correctly during the upgrade.

Procedure

1. Before you upgrade, SSH to the RealPresence DMA system as root and execute the following command from the shell:

   ```bash
   sed -i -e 's!${PROMPTS_DIR:-"/proximo/config/cluster"}!${PROMPTS_DIR:-"/proximo/config/promptsets"}!' /proximo/current/bin/backup_scripts/sys-backup-restore
   ```

2. Upgrade the system.

Upgrading the RealPresence Access Director System

You can upgrade version 4.2.x of the RealPresence Access Director system to version 10.0.x of the RealPresence DMA system.

The upgrade process migrates the RealPresence Access Director SSH passwords for the following user accounts to the RealPresence DMA system:

- polycom
- root
- rpad (The rpad user is converted to the dmaremote user but the password remains the same.)

Upgrade a RealPresence Access Director System

You can upload a RealPresence DMA software upgrade package and install the upgrade on your RealPresence Access Director system.

Download a recent backup file or take a snapshot of your Virtual Edition instance.

Open port 8443 on your internal firewall. A RealPresence DMA edge system uses port 8443 on the physical interface to connect to a core system for registration sharing.

Disable High Availability (HA) on both systems before you upgrade a RealPresence Access Director HA pair.

The upgrade process migrates the RealPresence Access Director system to a RealPresence DMA edge system.

Procedure

1. Log into Polycom Support.
2. Go to Documents and Software.
3. In the Product/Category list, select UC Infrastructure.
4. Select Management & Scheduling > RealPresence Distributed Media Application (DMA).
5. In the Current Releases tab, download one of the following upgrade files:
   - If you upgrade from version 4.2.0 through 4.2.5, download the `.upg` file.
If you upgrade from version 4.2.5.1 or later, download either the .upg file or .bin file.

6. Read and accept the End User License Agreement and the Export Restrictions.
7. Save the upgrade package to your local client system.
8. From the RealPresence Access Director system web interface, go to Maintenance > Software Upgrade.
10. Go to the upgrade package you saved and select Open.
11. Select Upgrade status page below the status bar.
    The RPP Install Status page displays. After the installation status reaches 100%, the system reboots.
12. After the system reboots, select **Click here to connect to DMA in Edge mode when the upgrade is complete** to display the RealPresence DMA login screen.
13. Using your administrator login credentials from the RealPresence Access Director system, log into the RealPresence DMA system web interface.
14. Read and accept the End User License Agreement.
    The system web interface opens and displays upgrade alerts.
15. Complete the following steps:
    - Go to Admin > Server > Network Settings and revise the System Ephemeral Ports to prevent overlap with the ports used for services (go to Service Config > System Port Ranges to view port assignments for services).
    - Go to Service Config > Call Server Settings > Registration Sharing Settings and enter the RealPresence DMA administrator user credentials.
    - If you upgraded HA systems, change the existing physical IP addresses for media interfaces to virtual IP addresses, then assign new physical IP addresses to the media interfaces.
16. Resolve any remaining upgrade alerts to complete the upgrade.

### Upgrade RealPresence Access Director Systems in a Two-Box Tunnel Configuration

If you have two RealPresence Access Director systems in a two-box tunnel configuration, you can upgrade them to RealPresence DMA systems with a VPN tunnel configuration.

Disable two-box tunnel mode on both RealPresence Access Director systems before you upgrade them to RealPresence DMA systems.

The upgrade process migrates each RealPresence Access Director system to a RealPresence DMA edge-configured system. The RealPresence Access Director system that resided in the DMZ remains in the DMZ as the outside RealPresence DMA edge system. You can configure the other migrated RealPresence Access Director system as an inside RealPresence DMA edge or combination system.

After you upgrade, the communication settings on the outside RealPresence DMA edge system point to the RealPresence DMA core system. You need to revise the settings so that external SIP peers, external H.323 gatekeepers, registration sharing, dial rules, and access proxies point to the inside edge or combination system. The same settings on the inside edge system must point to the RealPresence DMA core system. If you configure the inside RealPresence DMA as a combination system, it doesn’t need to point to a core system.

**Procedure**

1. Disable two-box tunnel mode on both RealPresence Access Director systems.
2. Upgrade both systems to RealPresence DMA systems.
3. On the outside RealPresence DMA edge system, do the following:
   - Point external SIP peers, external H.323 gatekeepers, registration sharing, and access proxies to the inside edge or combination system.
   - Assign standard ports to the HTTPS, LDAP, and XMPP proxies on the public side.
   - Assign non-standard ports to the HTTPS, LDAP, and XMPP proxies on the private side.

4. On the inside RealPresence DMA edge or combination system, do the following:
   - Assign non-standard ports (the same ones you assigned to the private side of the outside system) to the HTTPS, LDAP, and XMPP proxies on the public side.
   - Assign standard ports to the HTTPS, LDAP, and XMPP proxies on the private side.
   - Create an external SIP peer and external gatekeeper that point to the signaling address of the outside edge system. This enables outbound calling through the VPN tunnel.

5. If the inside RealPresence DMA is an edge-configured system, point external SIP peers, external H.323 gatekeepers, registration sharing, and access proxies to the core system.

Verify and Revise RealPresence DMA Edge System Settings

After you upgrade RealPresence Access Director single or two-box tunnel systems to the RealPresence DMA system, you need to verify that the configuration settings migrated correctly. You also need to revise some of the RealPresence DMA system’s settings.

RealPresence Access Director licenses won’t migrate and can’t be applied to a RealPresence DMA edge system. However, calls through the unlicensed edge system will continue to work if the edge system communicates with a core system. Adding licenses to an edge system for concurrent calls and concurrent VMRs is optional.

Procedure

1. Go to Admin > Server > Network Settings.
2. Select Services and verify that the services mapping is the same as it was in the RealPresence Access Director system.
3. In Network Interface Settings, do the following:
   a. Select an interface.
   b. Select the Edit button.
   c. Select IPv4 Configuration and verify the NAT address for the interface.
   d. Repeat for each interface.
4. Go to Admin > Server > Certificates and verify that your signed certificates are installed. Reinstall if necessary.
5. Go to Service Config > Access Control and verify that the ACL Variables, ACL Rules, and ACL Settings are correct. If not, edit or create new variables, rules, and settings as needed.
6. Go to Service Config > SIP Settings and do the following:
   a. Select a port.
   b. Select the Edit button.
   c. Select Factory Core Registration Policy as the default registration policy.
   d. Repeat for all SIP ports to enable calling from non-provisioned SIP endpoints.
7. Go to Service Config > H.323 Settings and do the following:
a. If your signaling service for Private and Public is on the same network interface, select By topology as the Policy Selection.

b. Select Factory Core Registration Policy as the Registration policy on both the Private and Public network interfaces to enable calling from non-provisioned H.323 endpoints.

8. Go to Service Config > Dial Plan > Domain Restrictions and add all local domains to enable SIP calls to work correctly.

9. Go to Service Config > Dial Plan > Dial Plans and do the following:

a. Select SIP Dial Plan Public and verify that the Resolve to external address dial rule points to the correct external SIP peer (the core RealPresence DMA system). If you have more than one core system in a supercluster, the dial rule should point to the embedded DNS name of the territory.

b. Select H.323 Dial Plan Public and verify that the Resolve to External H.323 Gatekeeper dial rule points to the correct external H.323 gatekeeper (the core RealPresence DMA system). If you have more than one core system in a supercluster, the dial rule should point to the embedded DNS name of the territory.

10. Go to Service Config > Site Topology > Sites and verify that the Default Site includes subnets for all RealPresence DMA systems in the supercluster.

Adjust Ports After Upgrading

You can adjust the port ranges for services and the system ephemeral ports after you upgrade the RealPresence DMA system.

After you upgrade, alerts for overlapping ports may display based on the system you upgraded (RealPresence Access Director or RealPresence DMA). To clear the alerts, you can adjust the system ephemeral ports and port range settings for services. You can shrink the port ranges of the services based on the number of call licenses you have.

Note: If you revise port ranges, keep the first port number the same and decrease the last port number. The total ports to reserve should match the formula in the following table. By using this method, you may not need to make network or firewall changes.

Procedure

1. In the system web interface, go to the location of the port range settings that you need to revise:
   - H.323 dynamic ports: Service Config > H.323 Settings
   - SIP dynamic ports: Service Config > SIP Settings
   - Media traversal dynamic ports: Service Config > Media Traversal Settings
   - Access proxy ports: Service Config > Access Proxy Settings
   - System ephemeral ports: Admin > Server > Network Settings

2. Use the formula described in the following table to calculate the required ports:
### Calculations for Number of Required Ports

<table>
<thead>
<tr>
<th>Information Type</th>
<th>H.323 Dynamic Ports</th>
<th>SIP Dynamic Ports (public)</th>
<th>SIP Dynamic Ports (private)</th>
<th>Media Traversal Dynamic Ports (public) (edge or combo config)</th>
<th>Media Traversal Dynamic Ports (private) (edge or combo config)</th>
<th>Access Proxy (edge or combo config)</th>
<th>System Ephemeral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports used per call</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>10</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Number of calls</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Total ports required</td>
<td>3x</td>
<td>3x</td>
<td>3x</td>
<td>10x</td>
<td>10x</td>
<td>3000</td>
<td>3000</td>
</tr>
</tbody>
</table>

3. Revise the port ranges as needed.

### Roll Back an Upgrade

When you upgrade the RealPresence DMA system, the upgrade process automatically creates a backup that you can use to roll back the upgrade if necessary.

You can roll back only the last applied upgrade. Rolling back an upgrade restores the database to its state before the upgrade, so data may be lost.

If a rollback is necessary, you may need to reconfigure supercluster or High Availability (HA) settings for your system(s).

Rolling back to a previous version terminates active calls and conferences and requires a system restart.

The following table describes the states of a RealPresence DMA system before and after an upgrade and after a rollback.

<table>
<thead>
<tr>
<th>System Version and State Before Upgrade</th>
<th>System State After Upgrade and Additional Configuration</th>
<th>System Version and State After Rollback</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.x - Standalone single-server cluster</td>
<td>Part of an HA pair or supercluster</td>
<td>9.0.x - Standalone single-server cluster</td>
</tr>
<tr>
<td>9.0.x - Part of an HA pair or supercluster</td>
<td>Part of an HA pair or supercluster</td>
<td>9.0.x - Part of an HA pair or supercluster</td>
</tr>
<tr>
<td>6.4.x - Standalone single-server cluster</td>
<td>Part of an HA pair or supercluster</td>
<td>6.4.x - Standalone single-server cluster; cannot pair or supercluster with 9.0.x systems.</td>
</tr>
<tr>
<td>6.4.x - Part of an HA pair or supercluster</td>
<td>Part of an HA pair or supercluster</td>
<td>6.4.x - Standalone single-server cluster; cannot pair or supercluster with 9.0.x systems; may be able to re-establish superclusters with 6.4.x systems but it's not guaranteed.</td>
</tr>
</tbody>
</table>
Procedure
1. Go to Admin > Software Upgrade.
2. Verify that you want to downgrade the system to the Rollback version shown.
3. Click Roll Back.
4. Click Yes to confirm the rollback.
   The system logs you out and restarts.
5. After the system restarts, log back into the management user interface.
6. Go to Admin > Software Upgrade and check the Operation History table to confirm the rollback was successful.

View Upgrade Information
The software upgrade page lists current version information, upgrade packages you have uploaded, and upgrade operation history.

Procedure
» Go to Admin > Software Upgrade to view the following upgrade details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version information</td>
<td>Shows the current system version and the rollback version (if any), which is the previous system version.</td>
</tr>
<tr>
<td>Upgrade package details</td>
<td>Shows the version number and other information about the upgrade file that's been uploaded (if any). Also indicates whether the system must be restarted after upgrading and displays a brief description, which includes an estimated install time.</td>
</tr>
<tr>
<td>Operation history</td>
<td>Lists each upgrade management operation (upgrade or downgrade), showing the server on which it was performed, package version, date of the operation, and which user performed it.</td>
</tr>
</tbody>
</table>
Shutting Down and Restarting

Topics:

- Restart or Shut Down One or Both Servers in a Cluster
- Start a Shut Down Cluster

The RealPresence DMA system's **Shutdown and Restart** page lets you restart the system or turn it off completely.

In a two-server cluster, you can shut down or restart either one or both servers in the cluster.

There's no mechanism for shutting down an entire supercluster at once. If you want to shut down all clusters in a supercluster, you must do so one cluster at a time. Wait at least 5 minutes before shutting down the next cluster.

If you want to shut down a cluster in the supercluster while other clusters remain on, remove the cluster from the supercluster, if it will remain shut down for more than a few hours. The supercluster retains only a limited amount of playback data that can be used to bring the shut-down cluster back up-to-date once it's turned back on. If the cluster remains off long enough, its data store cannot be made consistent with the rest of the supercluster.

Both shutting down and restarting will terminate all existing calls and log out all current users.

---

**Note:** Do not turn off a RealPresence DMA system server by unplugging it, especially if it's going to remain off for some time. If a server loses power without being properly shut down, the RAID controller fails to shut down, eventually depleting the server's battery. If that happens, the server cannot be restarted without user input, requiring a keyboard and monitor.

---

**Restart or Shut Down One or Both Servers in a Cluster**

From the **Shutdown and Restart** page, you can restart or shut down one or both servers in a cluster.

To shut down all clusters in a supercluster, repeat the following procedure on each additional cluster, waiting at least 5 minutes between clusters.

**Procedure**

1. Go to **Admin > Shutdown and Restart**.
   
   The page displays the server or servers in the cluster, along with status information.

2. Select the server(s) you want to shut down or restart.

3. Do one of the following:
   
   - To restart the selected server(s), click **Restart**.
   - To shut down the selected server(s), click **Shut Down**.

4. When asked to confirm that you want to restart or shut down, click **Yes**.

   The system logs you out and the selected server(s) shut down. If you choose **Restart**, the servers reboot and the conference service becomes available again when the restart is complete. If you choose **Shut Down**, the servers remain powered off until you manually turn them back on.
Start a Shut Down Cluster

Follow this procedure to start a cluster that has been shut down.

To start all clusters in a supercluster, repeat the following procedure on each additional cluster, waiting at least 5 minutes between clusters. After all clusters have restarted, it may take up to 30 minutes for all supercluster-wide replication to complete.

Procedure

1. Turn on the first server in the cluster.
   The server boots, which takes several minutes.
2. Wait at least one minute and turn on the second server in the cluster.
   The second server boots. When done, the LCDs of both the servers display **DMA Clustered** (applies to Polycom Rack Server 640, 630, or 620-based systems only).
Monitoring

Topics:

- Active Calls
- Endpoints
- High Availability Status
- Login Sessions
- Site Statistics
- Site Link Statistics
- SNMP Monitoring

This section provides an introduction to monitoring the Polycom RealPresence DMA system.
Active Calls

Topics:

- Search for Active Calls
- View Call Details

From the Active Calls page, you can monitor the calls in progress (managed by the RealPresence DMA call server) and disconnect an active call.

Search for Active Calls

The search feature enables you to find active calls matching the criteria you specify.

You can limit your search by specifying one or more of the following:

- Originator and/or destination device by its name, alias, or IP address
- Cluster, territory, or site name
- Signaling type or registration status
- Class of service or bit rate range

The system matches any string you enter against the beginning values of active call fields. If you enter 10.33.17 as an originator IP address, the system displays calls from devices whose IP addresses are in that subnet. To search for a string not at the beginning of a field, you can use an asterisk (*) as a wildcard.

Leave a field empty (or select the blank entry from a list) to match all values.

The calls that match your search criteria display in the Active Calls list. You can pin a call that you want to review. This moves it to the Pinned Calls list and it remains there, even after the call ends, until you unpin it.

Details about the selected call are available in the Call Info, Originator, Destination, and Bandwidth drop-down lists. This information (and more) is also available in Call Details dialog, which appears when you click Show Call Details (in the Actions list).

Procedure

1. Go to Monitoring > Active Calls.
2. Enter the Dial String to search for or click the filter button for more search options.
3. Select the filters you want and enter search strings for one or more fields (optional).
   - Leave a filter's field empty to match all values for that filter.
4. Click Search to display the active calls that match your search criteria.

View the Active Calls List

The RealPresence DMA Active Calls list displays all calls currently in progress.

You can pin a call that you want to review. This moves it to the Pinned Calls list and it remains there, even after the call ends, until you unpin it.
RealPresence DMA core systems also display calls that are active on an integrated edge system (or other core system in a VPN tunnel) that doesn’t have call licenses. However, not all call details display on the core system. To see complete call details, view them from the edge or other core system.

**Procedure**

» Go to Monitoring > Active Calls.

The following table describes the columns in the **Active Calls** list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Pin state)</td>
<td>Click to pin a call, moving it to the <strong>Pinned Calls</strong> list and keeping its information available even if the call ends. Click again to unpin it.</td>
</tr>
<tr>
<td>Start time</td>
<td>Time the call began (first signaling event).</td>
</tr>
<tr>
<td>Originator</td>
<td>Source of the call (the device's display name, if available; otherwise, its name, alias, or IP address, in that order of preference). If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>Dial string</td>
<td>Dial string sent by the originator, when available.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination of the call (the device's display name, if available; otherwise, its name, alias, or IP address, in that order of preference). If the destination is an MCU, the MCU name.</td>
</tr>
<tr>
<td>Bit rate</td>
<td>Bit rate (kbps) of the call. A down arrow indicates that the call was downspeeded. Hover over it to see details.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Class of service of the call, Gold, Silver, or Bronze.</td>
</tr>
</tbody>
</table>

**View Call Details**

You can view a call’s details, which provide specific information about the selected call.

Note that some of the **Call Server Settings** can affect the values reflected for a call.

A fully-external call is a call that the RealPresence DMA system monitors and for which it has an audit record. However, a fully-external call's signaling does not pass through the RealPresence DMA system so these calls do not have signaling diagrams.

**Procedure**

1. Go to Monitoring > Active Calls.
2. Select the call of interest and click **Show Call Details** to display the following information:

<table>
<thead>
<tr>
<th>Tab/Field/Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Info</td>
<td></td>
</tr>
<tr>
<td>Tab/Field/Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Call info        | Displays the call's:  
|                  | • Status (active/ended and pinned/unpinned)  
|                  | • Start time and end time  
|                  | • Duration  
|                  | • Signaling protocol(s)  
|                  | • RealPresence DMA server(s) involved  
|                  | • Unique call ID  
|                  | • Dial string, if available  
|                  | • Final dial string (after processing by dial rules)  

| Originator       | Displays the source device's:  
|                  | • Name and authentication name  
|                  | • Authentication status  
|                  | • Model and version  
|                  | • Aliases  
|                  | • IP address or host name  
|                  | • Registration status  
|                  | • Site and territory  

If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.

| Destination      | Displays the destination device’s:  
|                  | • Name and authentication name  
|                  | • Authentication status  
|                  | • Model and version  
|                  | • Aliases  
|                  | • IP address or host name  
|                  | • Registration status  
|                  | • Site and territory  

If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.
### Tab/Field/Column | Description
--- | ---
**Bandwidth** | Available only after the call has ended. The table at the top lists each throttle point that the call traverses and shows its:
  - Bit rate limit per call (kbps)
  - Total capacity (kbps)
  - Used bit rate (kbps) in each class of service
  - Weight (%)
  - Territory

If the throttle point is a subnet, site, or site link, a link takes you to the corresponding site topology page with the throttle point entity selected.

Below the table, the data used in bandwidth processing displays (all bit rates are kbps):
  - **Formal maximum bit rate limit** - the maximum allowed bit rate considering the per call bit rates of each throttle point, but not considering total capacity or current usage
  - Available bit rate capacity in each class of service and for the call's class
  - Class of service for the call
  - Minimum downspeed bit rate
  - **Available bit rate limit (%)** - the maximum percentage of remaining bandwidth at a throttle point that will be given to any one call (configurable in **Call Server Settings**)
  - Requested bit rate
  - Final bit rate

**Call events** | Lists each call event in the call and its attributes.

When the system is operating as a SIP proxy server, the list includes all SIP signaling messages except 100 TRYING.

Hover over an attribute label to see a description. Click **Show Message** to see the signaling message. Click **Show QoS Data** to see detailed Quality of Service statistics.

**Subscription events** | For conference (VMR) calls, lists SUBSCRIBE/NOTIFY events, if any, associated with this call.

The **SIP SUBSCRIBE/NOTIFY** conference notification service allows SIP devices (generally, conference participants) to subscribe to a conference and receive conference rosters and notifications of conference events. The rosters identify the participants, their endpoints, and their video streams.

Hover over an attribute label to see a description.

**Note:** If the system is configured to allow devices to subscribe to a conference without being participants in the conference, the call history doesn't include data for such non-participant subscriptions. However, a subscription to a conference by a non-participant consumes a call license.
<table>
<thead>
<tr>
<th>Tab/Field/Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property changes</td>
<td>Lists each property change in the call, showing the value, time, and sequence number of the associated event.</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of service (QoS) data is only available if one of the endpoints is a registered H.323 endpoint that supports IRQs. This tab displays a graph showing how QoS varied during the call. The horizontal scale and frequency of data points (dots on the lines of the graph) vary based on the length of the call. Hover over a data point to see the value at that point.</td>
</tr>
</tbody>
</table>
| Signaling diagram     | This tab displays a diagram showing the sequence of signaling events during the call. The image lists signaling events from the endpoints, MCUs, and any RealPresence DMA system(s) involved in the call (more than one cluster may be represented if using a superclustered configuration). The header for each column is labeled with the device name, its IP address, and the signaling port. Click on a **signaling message** or **call property change** to view details about that message or property change. Each signaling message is labeled with the message time, sequence number, and message type. The sequence number matches the sequence number for the event in the call events tab. Click **Download Image** to save a copy of the call events diagram to your PC. Click **Download Call Events (XML)** to save the call event details in XML format.**Note:** Fully external calls, whose signaling does not pass through the RealPresence DMA system, have no signaling diagrams.
Endpoints

Topics:

- Search for Endpoints
- Add an Endpoint
- Edit an Endpoint
- Edit Multiple Endpoints
- Delete an Endpoint
- Add an Alias
- Edit an Alias
- Associate a User with an Endpoint
- Disassociate a User from an Endpoint
- Block Registrations from an Endpoint
- Unblock Registrations from an Endpoint
- Quarantine an Endpoint
- Unquarantine an Endpoint
- View Call History
- View Registration History
- Names and Aliases in a Mixed H.323 and SIP Environment
- Naming ITP Systems for Recognition by the RealPresence DMA System

The RealPresence DMA system integrates with endpoint devices to support videoconferencing. You can monitor and manage endpoints from your system's management interface.

Search for Endpoints

You can find endpoints you need to monitor based on various search criteria.

Procedure

1. Go to Monitoring > Endpoints.
   
   The search field above the list of endpoints enables you to find devices matching the criteria you specify. The default search finds all endpoints with active registrations.

2. To view all endpoints, regardless of registration status, click the filter button next to the Name field and turn off Registration status as one of the search criteria.

3. Click Search to display all endpoints.
   
   The following table describes the information that displays in the Endpoints list.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>Model</td>
<td>The model designation of the device.</td>
</tr>
<tr>
<td>IP address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>Alias</td>
<td>The aliases, if any, assigned to the device.</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the device belongs.</td>
</tr>
<tr>
<td>Owner domain</td>
<td>The domain to which the device's owner, if any, belongs.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who owns the device.</td>
</tr>
<tr>
<td>Class of service</td>
<td>The class of service assigned to the device:</td>
</tr>
<tr>
<td></td>
<td>▪ Gold</td>
</tr>
<tr>
<td></td>
<td>▪ Silver</td>
</tr>
<tr>
<td></td>
<td>▪ Bronze</td>
</tr>
<tr>
<td></td>
<td>▪ Inherit from associated user (if none, default to Bronze)</td>
</tr>
<tr>
<td>Note:</td>
<td>The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Admission policy</td>
<td>Indicates the admission policy applied to the device:</td>
</tr>
<tr>
<td></td>
<td>▪ Allow</td>
</tr>
<tr>
<td></td>
<td>▪ Block</td>
</tr>
<tr>
<td></td>
<td>▪ Quarantine</td>
</tr>
<tr>
<td></td>
<td>▪ Reject</td>
</tr>
<tr>
<td>Compliance level</td>
<td>Indicates whether the device is compliant or non-compliant with the applicable registration policy script.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registration status</td>
<td>The registration status of the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong> - The device is registered and can make and receive calls.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inactive</strong> - The device's registration has expired. Whether it can make and receive calls depends on the system's rogue call policy in <strong>Call Server Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quarantined</strong> - The device is registered, but it cannot make or receive calls. It remains in Quarantined or Quarantined (Inactive) status until you remove it from quarantine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quarantined (Inactive)</strong> - The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blocked</strong> - The device is not permitted to register. It remains blocked from registering until you unblock it.</td>
</tr>
</tbody>
</table>

If the device is in a site managed by the system, its ability to make and receive calls depends on the system’s rogue call policy.

If the device is not in a site managed by the system, it can’t make or receive calls.

A device’s status can be determined by:

• An action by the device.
• An action applied to it manually on this page.
• The expiration of a timer.
• The application of a registration policy and admission policy.

<table>
<thead>
<tr>
<th>Exceptions</th>
<th>Shows any exceptions returned for a device as a result of applying a registration policy script.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active calls</td>
<td>Indicates if the device is in a call.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the endpoint must authenticate itself.</td>
</tr>
<tr>
<td>Note:</td>
<td>Inbound authentication for the device type must be enabled at the system level, or the setting for the device has no effect.</td>
</tr>
</tbody>
</table>

4. For more search options, click the filter button to the right of the Name field.

5. Select the filters you want and enter search strings for one or more fields.

6. Click Search.

The system matches any string you enter against the beginning of the values for which you entered it. If you enter 10.33.17 in the IP address field, it displays devices whose IP addresses are in that subnet. To search for a string not at the beginning of the field, you can use an asterisk (*) as a wildcard.
Add an Endpoint

You can manually add an endpoint to the system.

When you do so, the system applies a registration policy script to determine if the device is compliant or non-compliant with the policy, and then applies the admission policy associated with that result to determine the registration status of the device.

Procedure

1. Go to Monitoring > Endpoints.
2. Click Add.
3. Complete the fields as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device type</td>
<td>The device's signaling protocol (H.323 or SIP).</td>
</tr>
<tr>
<td>Signaling address</td>
<td>For an H.323 device, the H.225 call signaling address and port of the device. Either this or the RAS address is required.</td>
</tr>
<tr>
<td>RAS address</td>
<td>For an H.323 device, the Registration, Admission and Status (RAS) channel address and port of the device.</td>
</tr>
<tr>
<td>Aliases</td>
<td>For an H.323 device, lists the device's aliases. When you add a device, this list is empty. The Add button lets you add an alias.</td>
</tr>
<tr>
<td>Address of record</td>
<td>For a SIP device, the AOR with which the device registers (see registration rules in RFC 3261), such as: sip:<a href="mailto:1000@westminster.polycom.com">1000@westminster.polycom.com</a></td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the endpoint must authenticate itself.</td>
</tr>
<tr>
<td>Note: Inbound authentication for the device type must be enabled at the system level or the setting for the device has no effect.</td>
<td></td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to specify the class of service and the bit rate limits for calls to and from this device.</td>
</tr>
<tr>
<td>A call between two devices receives the higher class of service of the two.</td>
<td></td>
</tr>
<tr>
<td>Note: The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.</td>
<td></td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>The maximum bit rate for calls to and from this device.</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which calls from this device can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped.</td>
</tr>
<tr>
<td>Model</td>
<td>Optional model number/name for the device.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional version information for the device.</td>
</tr>
</tbody>
</table>

4. Click OK.
Edit an Endpoint

You can change a device's class of service setting, add aliases, and edit or delete added aliases. You cannot edit or delete aliases with which the device registered.

Procedure

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the device to edit.
4. Click Edit.
5. Revise the editable fields as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the H.323 or SIP device. For an H.323 device, the name is the Alias Value of the most-recently added alias. Display only.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of the endpoint, if known. Display only.</td>
</tr>
<tr>
<td>Aliases</td>
<td>For an H.323 device, lists the device's aliases. When you edit a device, you can edit or delete an existing alias, or add a new alias.</td>
</tr>
<tr>
<td>Site</td>
<td>The site to which the device belongs. Display only.</td>
</tr>
<tr>
<td>Owner domain</td>
<td>The domain to which the device's owner belongs, if provided by the device. Display only.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who owns the device, if provided by the device. Display only.</td>
</tr>
<tr>
<td>Registration status</td>
<td>The registration status of the device. Display only.</td>
</tr>
<tr>
<td>Permanent</td>
<td>When selected, prevents the registration from ever expiring.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the endpoint must authenticate itself.</td>
</tr>
<tr>
<td></td>
<td>Note: Inbound authentication for the device type must be enabled at the system level, or the setting for the device has no effect.</td>
</tr>
<tr>
<td>Class of service</td>
<td>Select to modify the class of service and the bit rate limits for calls to and from this device. A call between two devices receives the higher class of service of the two. Note: The class of service of the device applies to point-to-point calls. VMR calls use the class of service of the conference room.</td>
</tr>
<tr>
<td>Maximum bit rate (kbps)</td>
<td>The maximum bit rate for calls to and from this device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimum downspeed bit rate (kbps)</td>
<td>The minimum bit rate to which calls from this device can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped.</td>
</tr>
<tr>
<td>Forward unconditional</td>
<td>Forward all calls to the specified alias. Registered endpoints can activate this feature by dialing the VSC for it (default is *75) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Forward busy</td>
<td>If the device is busy, forward calls to the specified alias. Registered endpoints can activate this feature by dialing the VSC for it (default is *74) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Forward no answer</td>
<td>If the device doesn't answer, forward calls to the specified alias. Registered endpoints can activate this feature by dialing the vertical service code (VSC) for it (default is *73) followed by the alias. They can deactivate it by dialing the VSC alone.</td>
</tr>
<tr>
<td>Alert when device unregisters</td>
<td>If the device unregisters from the call server or its registration expires, an informational alert is triggered (alert 5003).</td>
</tr>
</tbody>
</table>

**Edit Multiple Endpoints**

When you select multiple endpoints, you can change certain settings for all of the selected endpoints at one time.

**Procedure**

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the device to edit.
   - Use Shift-click or Ctrl-click to select one or more additional endpoints.
4. Click Edit.
5. Complete the fields in the Edit Endpoints window as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permanent</td>
<td>Prevents the registration of the selected devices from ever expiring.</td>
</tr>
<tr>
<td>Device authentication</td>
<td>Indicates whether the selected devices must authenticate themselves. * Inbound authentication for the device type must be enabled at the system level or the setting for these devices has no effect.</td>
</tr>
</tbody>
</table>
### Field Description

**Class of service**
Select to modify the class of service and the bit rate limits for calls to and from the selected devices.

A call between two devices receives the higher class of service of the two.

* The class of service of the device applies to point to point calls. VMR calls use the class of service of the conference room.

**Maximum bit rate (kbps)**
The maximum bit rate for calls to and from the selected devices.

**Minimum downspeed bit rate (kbps)**
The minimum bit rate to which calls from the selected devices can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped.

**Alert when device unregisters**
If one of the selected devices unregisters from the call server or its registration expires, an informational alert is triggered (alert 5003).

---

6. Click OK.

**Related Links**

[Device Authentication](#) on page 408

---

## Delete an Endpoint

You can delete one or more inactive endpoints from the RealPresence DMA system.

An inactive device is one whose registration has expired. Depending on your [Registration Policy](#) settings, inactive devices may be automatically deleted after a specified number of days.

**Procedure**

1. Go to **Monitoring > Endpoints**.
2. Enter the search criteria you want and click **Search** to display endpoints that match your criteria.
3. Select the device to delete.
4. Click **Delete**.
5. Click **Yes** to confirm the deletion.

---

## Add an Alias

You can specify an alias for an H.323 device that you add or edit.

To specify an alias:

**Procedure**

1. Go to **Monitoring > Endpoints**.
2. Do one of the following:
   - Click the **Add** button.
   - Search for an endpoint, select it from the list, and click **Edit**.
3. In the **Aliases** section, click the **Add** button.
4. Enter the alias in the **Value** field and click **OK**.
Edit an Alias

You can revise an existing alias that you’ve added for an H.323 device. You cannot edit an alias that a device used to register.

To revise an existing alias:

Procedure

1. Go to Monitoring > Endpoints.
2. Search for and select the endpoint with the alias you want to edit.
3. Click the Edit button.
4. In the Aliases section, select the alias to edit.
5. Click the Edit button.
6. Revise the alias in the Value field as needed and click OK.
7. Click OK to close the Edit Endpoint window.

Associate a User with an Endpoint

You can associate a user with an endpoint by selecting the endpoint, then searching for the user with whom to associate it.

You can search by First name, Last name, and/or User ID. The Search users field searches all three for matches.

Note that the system matches the string you enter against the beginning of the field you are searching. For example, if you enter sa in the Last name field, the search results display users whose last names begin with sa. To search for a matching string not at the beginning of the field, you can use an asterisk (*) as a wildcard, such as *sa.

Procedure

1. Go to Monitoring > Endpoints.
2. Select the endpoint to associate with a user.
3. Click Associate User.
4. Enter the search criteria you want and click Search to display users that match your criteria.
5. Select the user to associate with the endpoint and click OK.
6. Click Yes to confirm the association.

The Owner column on the Endpoints page displays the user associated with the endpoint.

Disassociate a User from an Endpoint

When necessary, you can disassociate a selected device from an associated user.

Procedure

1. Go to Monitoring > Endpoints.
2. Search for and select the endpoint to disassociate from a user.
3. Click Disassociate User.
4. Click Yes to confirm the disassociation.
Block Registrations from an Endpoint

Blocking a device prevents it from registering with the RealPresence DMA system.

Procedure
1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to block from registering with the RealPresence DMA system.
   - Use Shift-click or Ctrl-click to select one or more additional endpoints to block.
4. Click Block Registrations.
5. Click Yes to confirm the block.

Unblock Registrations from an Endpoint

Unblocking a blocked device allows it to register with the RealPresence DMA system.

Procedure
1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to unblock from registering.
   - Use Shift-click or Ctrl-click to select one or more additional endpoints to unblock.
4. Click Unblock Registrations.
5. Click Yes to confirm that you want to unblock the endpoint from registering.

Quarantine an Endpoint

When you quarantine an endpoint, it can register (or remain registered) with the RealPresence DMA system, but cannot make or receive calls.

Procedure
1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to quarantine.
   - Use Shift-click or Ctrl-click to select one or more additional endpoints to quarantine.
4. Under Actions, click Quarantine.
5. Click Yes to confirm the quarantine.

Unquarantine an Endpoint

When you remove an endpoint from quarantine, it can once again register with the RealPresence DMA system and make and receive calls.
Procedure

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint to unquarantine.
   - Use Shift-click or Ctrl-click to select one or more additional endpoints to unquarantine.
4. Click Unquarantine.
5. Click Yes to confirm the removal from quarantine.

View Call History

When you view the call history for an endpoint, the RealPresence DMA system displays the Call History page, where you can export CDR data and search results, show export history, and show call details.

Procedure

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint whose call history you want to view.
4. Click View Call History.
   - The Call History page displays.

Related Links
Call History on page 549

View Registration History

When you view the registration history for an endpoint, the RealPresence DMA system displays the Registration History page, where you can view registration details of a selected endpoint.

Procedure

1. Go to Monitoring > Endpoints.
2. Enter the search criteria you want and click Search to display endpoints that match your criteria.
3. Select the endpoint whose registration history you want to view.
4. Click View Registration History.
   - The Registration History page displays.

Names and Aliases in a Mixed H.323 and SIP Environment

An endpoint that supports both H.323 and SIP can register with the RealPresence DMA system’s gatekeeper and SIP registrar using the same name/alias.

When the RealPresence DMA system receives a call for that endpoint, it uses the protocol of the calling endpoint. This can lead to failed calls under the following circumstances:

- The system is configured to allow calls to/from rogue (not actively registered) endpoints.
An endpoint that was registered with both protocols (using the same name/alias) later has one of the protocols disabled, and that registration expires (or otherwise becomes inactive).

The RealPresence DMA system is not aware if an endpoint no longer supports a protocol. When another endpoint tries to call using the called endpoint’s disabled protocol, the system still tries to reach it using that protocol, and the call fails.

To avoid this problem, you can do one of the following:

- Ensure that endpoints supporting both protocols use different names/aliases for each protocol.
- Do not allow calls to/from rogue endpoints.
- If you know that an endpoint has stopped supporting a protocol, manually delete its inactive registration for that protocol.

Related Links

Configure the Call Server on page 297

---

**Naming ITP Systems for Recognition by the RealPresence DMA System**

A RealPresence DMA Immersive Telepresence (ITP) room system contains multiple displays and codecs (endpoints).

If the ITP system is using SIP or H.323 signaling (not Cisco TIP signaling), the RealPresence DMA system will recognize the endpoints as part of an ITP system only if they have names that properly identify them. The names must take the form `systemName_M_N`, where `M` is the total number of displays in the ITP system (2, 3, or 4) and `N` is the sequence number of each display. The primary codec must be assigned sequence number 1.

For example, the three HDX devices in a Polycom OTX 300 ITP system named Bainbridge might be named as follows:

Bainbridge ITP_3_1 Bainbridge ITP_3_2 Bainbridge ITP_3_3

When these three devices register with the RealPresence DMA system's call server, the RealPresence DMA system recognizes them as a single ITP system and assigns them a Gold class of service (you can change this if necessary). The RealPresence DMA system also manages the device authentication settings as applying to a single system.

For ITP systems using SIP or TIP signaling (but not H.323), the RealPresence DMA system also creates a single CDR for calls from the ITP system rather than separate CDRs for each of the three devices.

You can only edit the device authentication and class of service settings for the primary codec; the RealPresence DMA system automatically propagates any changes to the other devices in the ITP system.

The RealPresence DMA system's ability to recognize ITP calls and treat them as one assures the same class of service and device authentication settings for all the endpoints in the ITP system, but not other registration settings. You need to ensure that the maximum and minimum bit rates and other registration settings are consistent.

Follow this naming convention for both the ITP system name and the name for each HDX endpoint in the ITP system. For more information, see the following documents:

- Administrator’s Guide for Polycom HDX Systems
- Polycom Immersive Telepresence (ITP) Deployment Guide
• Polycom Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions

Related Links
Alert 5001 on page 593
High Availability Status

Topics:

- Monitor High Availability Status
- Release Resources

If you have Polycom systems configured in High Availability (HA) mode, you can monitor the status of the HA pair from the management user interface.

Monitor High Availability Status

You can monitor the status of an HA pair, including network connections, virtual IP address activity, and connection status of the local node.

Procedure

» Go to Monitoring > High Availability Status.

The following HA status information displays:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Status</strong></td>
<td></td>
</tr>
<tr>
<td>High availability status/mode</td>
<td>Specifies if High Availability mode is enabled or disabled and displays the HA mode (Active:Active or Active:Passive).</td>
</tr>
<tr>
<td>Local</td>
<td>Indicates whether the local node is connected to the network.</td>
</tr>
<tr>
<td>Peer</td>
<td>Indicates whether the peer node is connected to the network.</td>
</tr>
<tr>
<td><strong>Virtual IP Address List</strong></td>
<td></td>
</tr>
<tr>
<td>Virtual IP</td>
<td>Each of the virtual IP addresses configured for the HA pair.</td>
</tr>
<tr>
<td>Services</td>
<td>The services assigned to the virtual IP address.</td>
</tr>
<tr>
<td>Owner</td>
<td>The owner of the virtual IP address, that is, the node on which the virtual IP address should be active (local or peer). The Active label is green if the virtual IP address is active on the network and owned by the system that should own it. The Active label is yellow during a failover.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies whether the virtual IP address is active.</td>
</tr>
<tr>
<td><strong>Local HA Link Status</strong></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Each network interface on the local node that's configured for HA communication with the peer.</td>
</tr>
<tr>
<td>Physical IP</td>
<td>The physical IP address of the network interface.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct link</td>
<td>Indicates if the network interface has a direct link to the same network interface on the peer.</td>
</tr>
</tbody>
</table>

### Release Resources

You can release the resources of both the locally owned HA node and the peer node, or only the peer node.

**Procedure**

1. From the **High Availability Status** page, select **Release Resources**.
2. Select the virtual IP addresses to release:
   - **Both peer and locally-owned VIPs**: if you only want to release your own VIPs (for example, if there was no failover, select this option)
   - **Only peer-owned VIPs**
3. Select **Force release now** if you want to immediately release resources.
   - Selecting this option will terminate all active calls.
4. Click **OK**.
Login Sessions

Topics:

- View Login Sessions
- Terminate a User's Login Session

You can view all active user login sessions on your RealPresence DMA system. If you’re an administrator, you can terminate login sessions when necessary.

Related Links
Configure Session Settings on page 485

View Login Sessions

You can monitor all active login sessions on your Polycom system.

Procedure

» Go to Monitoring > Login Sessions.

The following login session information displays:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain/User name</td>
<td>The domain to which the user belongs.</td>
</tr>
<tr>
<td>Client platform</td>
<td>The platform from which the user logged in. The column provides details about the browser used to connect to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Client address at login time</td>
<td>The IP address from which the user logged in.</td>
</tr>
<tr>
<td>Age</td>
<td>The length of the login session in minutes.</td>
</tr>
<tr>
<td>Creation time</td>
<td>The time and date when the user logged in.</td>
</tr>
<tr>
<td>Server name</td>
<td>The host name of the server that the user logged in to.</td>
</tr>
</tbody>
</table>

Terminate a User's Login Session

You can terminate a user's login session manually in the Login Sessions page.

Procedure

1. Go to Monitoring > Login Sessions.
2. In the Login Sessions list, select the login session you want to terminate.
3. Click Terminate Session.
4. Click Yes to confirm.
The system terminates the session immediately and informs the user that the connection to the server was lost.
Site Statistics

The Site Statistics page lists the sites defined in the RealPresence DMA system's site topology. It also lists traffic and QoS statistics for sites controlled by the RealPresence DMA system. Network clouds and the default Internet site are not included.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Number of calls</td>
<td>Number of active calls on this site.</td>
</tr>
<tr>
<td>Bandwidth used %</td>
<td>Percentage of available bandwidth in use for this site.</td>
</tr>
<tr>
<td>Bandwidth (bps)</td>
<td>Total bandwidth in use for this site.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system uses the value of the Bit rate to bandwidth conversion factor in Call Server Settings to calculate the bandwidth in use.</td>
</tr>
<tr>
<td>Avg bit rate (bps)</td>
<td>Average bit rate of this site's active calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system uses the value of the Bit rate to bandwidth conversion factor in Call Server Settings to calculate the average bit rate.</td>
</tr>
<tr>
<td>Packet loss %</td>
<td>Average packet loss percentage of the site's active calls.</td>
</tr>
<tr>
<td>Avg jitter (msec)</td>
<td>Average jitter rate of the site's active calls.</td>
</tr>
<tr>
<td>Avg delay (msec)</td>
<td>Average delay rate of the site's active calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the site belongs.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Cluster responsible for the territory to which the site belongs.</td>
</tr>
</tbody>
</table>
The Site Link Statistics page lists the site links defined in the RealPresence DMA system's site topology. It also lists traffic and QoS statistics for site links controlled by the RealPresence DMA system. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site link name</td>
<td>Name of the site.</td>
</tr>
<tr>
<td>Number of calls</td>
<td>Number of active calls on this site.</td>
</tr>
<tr>
<td>Bandwidth used %</td>
<td>Percentage of available bandwidth in use for this site.</td>
</tr>
<tr>
<td>Bandwidth (bps)</td>
<td>Total bandwidth in use for this site.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system uses the value of the Bit rate to bandwidth conversion factor in Call Server Settings to calculate the bandwidth in use.</td>
</tr>
<tr>
<td>Avg bit rate (bps)</td>
<td>Average bit rate of this site's active calls.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The system uses the value of the Bit rate to bandwidth conversion factor in Call Server Settings to calculate the bandwidth in use.</td>
</tr>
<tr>
<td>Packet loss %</td>
<td>Average packet loss percentage of this site's active calls.</td>
</tr>
<tr>
<td>Avg jitter (msec)</td>
<td>Average jitter rate of this site's active calls.</td>
</tr>
<tr>
<td>Avg delay (msec)</td>
<td>Average delay rate of this site's active calls.</td>
</tr>
<tr>
<td>Territory</td>
<td>Territory to which the site belongs.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Cluster responsible for the territory to which the site belongs.</td>
</tr>
</tbody>
</table>
SNMP Monitoring

Topics:

- SNMP Framework
- SNMP Versions
- SNMP Notifications
- Configure SNMP Settings
- Notification Settings
- Security Users
- Download MIBs

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

SNMP provides a standardized framework and a common language used for the monitoring and management of resources in a network.

SNMP Framework

The SNMP framework has three parts:

- An SNMP manager
  The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. A variety of network management applications are available for use with SNMP. You should understand how your SNMP management system is configured to properly configure your RealPresence DMA system SNMP requirements, including transport protocol, version, authentication, and privacy. For information on using SNMP management systems, see the appropriate documentation for your application.

- An SNMP agent
  The SNMP agent is the software component within the RealPresence DMA system that maintains the data for the system and reports the data, as needed, to managing systems. The agent and MIB reside on the same system.

- A MIB
  The management information base (MIB) is a virtual information storage area for network management information, which consists of collections of managed network objects. You can configure the SNMP agent for a particular system MIB. The agent gathers data from the MIB, the repository for information about system parameters and network data. Polycom systems include Polycom-specific MIBs as well as third-party MIBs. Polycom MIBs are self-documenting, meaning they include information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system may include both hardware and software system MIBs.
SNMP Versions

Polycom supports two versions of SNMP:

- **SNMPv2c** - Polycom implements a sub-version of SNMPv2. SNMPv2c uses a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by an IP-based Access Control List and password.
  
  SNMPv2c does not encrypt communications between the management system and SNMP agents and is subject to packet sniffing of the clear text community string from the network traffic.

- **SNMPv3** - SNMPv3 provides secure access to systems by authenticating and encrypting packets over the network. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity. The `contextEngineID` is used to generate the key for authenticated messages. Polycom implements SNMPv3 communication with authentication and privacy (the authPriv security level as defined in the USM MIB).
  
  - Authentication is used to ensure that traps are read only by the intended recipient. As messages are created, they are given a special key that is based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.
  
  - Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.
  
  - Message integrity ensures that a packet has not been tampered with in transit.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent.

The RealPresence DMA system sends notifications, unsolicited and asynchronous, to the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to another system, or other significant events. They are generated as inform or trap requests.

Traps are messages alerting the SNMP manager to a system or network condition change. Informs are traps that include a request for a confirmation receipt from the SNMP manager. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. However, informs consume more system and network resources. Traps are discarded as soon as they are sent. An inform request is held in memory until a response is received or the request times out. Traps are sent only once while informs may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and informs provide a trade-off between reliability and network resources.

Configure SNMP Settings

Configure the RealPresence DMA SNMP **Agent Setting** first, then add security users and notification listeners as needed.

**Procedure**

1. Go to **Admin > Server > SNMP Settings**.
2. Select **Enable SNMP monitoring**.
3. Configure the following settings for the connection between the RealPresence DMA system and the SNMP agent:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SNMP version** | Specifies the version of SNMP you want to use.  
  v2c - Used for standard models. Uses community-based authentication.  
  v3  - Used when you want a high security model. Requires a security user for notifications. |
| **Transport**    | Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols:  
  TCP - This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP.  
  UDP - This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent. Because UDP does not have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring. |
| **Port**         | Specifies the port that the RealPresence DMA system uses to send SNMP messages.  
  Default port is 161 for UDP or TCP. |
| **Community**    | For SNMPv2c, specifies the context for the information, which is the SNMP group to which the devices and management stations running SNMP belong.  
  The RealPresence DMA system uses only the public context and will not respond to requests from management systems that do not belong to its community. |
| **Contact**      | The contact information for the SNMP agent. This may be a name, role, or other identifying information. |
| **Location**     | The physical location of the RealPresence DMA system. |
| **Local engine ID** | For SNMPv3 only.  
  Displays the RealPresence DMA system `contextEngineID` for SNMPv3. |
| **Security user** | For SNMPv3 only.  
  Specifies the security name required to access a monitored MIB object.  
  This name cannot be `snmpuser`. |

4. Click **Update**.
Notification Settings

In Notification Settings, you can specify the notification listeners (agents) and the types of notifications an agent sends to the RealPresence DMA system.

Add a Notification Listener

A notification listener sends SNMP messages to the RealPresence DMA system.

To limit the effect on system performance, you can add a maximum of eight notification listeners.

Procedure

1. Go to Admin > Server > SNMP Settings.
2. Under Notification Setting, click the Add button.
3. In the Add Notification Listener window, configure the settings described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification listener. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications from the listening agent. (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the listening agent that sends SNMP notifications to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the listening agent uses to send notifications to the RealPresence DMA system. Default port is 162 for UDP or TCP.</td>
</tr>
<tr>
<td>Notification type</td>
<td>The type of notification that this listening agent sends to the RealPresence DMA system:</td>
</tr>
<tr>
<td></td>
<td>• Inform - The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.</td>
</tr>
<tr>
<td></td>
<td>• Trap - The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>The version of SNMP used by this agent (v2c or v3).</td>
</tr>
<tr>
<td>Security user</td>
<td>For SNMPv3, the user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>

4. Click OK.

The notification listener displays in the Notification Setting list.

5. Select the Minimum recurring notification interval from the drop-down list.

6. Click Update to save the settings.
Edit a Notification Listener

Revise notification listeners as needed when settings change.

Procedure

1. Go to Admin > Server > SNMP Settings.
2. From the Notification Setting list, select the notification listener to edit.
3. Click the edit button.
4. Revise the following settings in the Edit Notification Listener window as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification listener. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications from the listening agent. (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the listening agent that sends SNMP notifications to the RealPresence DMA system.</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the listening agent uses to send notifications to the RealPresence DMA system. Default port is 162 for UDP or TCP.</td>
</tr>
<tr>
<td>Notification type</td>
<td>The type of notification that this listening agent sends to the RealPresence DMA system:</td>
</tr>
<tr>
<td></td>
<td>• Inform - The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.</td>
</tr>
<tr>
<td></td>
<td>• Trap - The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>The version of SNMP used by this agent (v2c or v3).</td>
</tr>
<tr>
<td>Security user</td>
<td>For SNMP v3, the user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>

5. Click OK to save the changes.
6. Select the Minimum recurring notification interval from the drop-down list.
7. Click Update to save the settings.

Delete a Notification Listener

Delete notification listeners if they’re no longer valid.

Procedure

1. Go to Admin > Server > SNMP Settings.
2. From the Notification Setting list, select the agent to delete
3. Click the Delete button.
4. Click Yes to confirm the deletion.
5. Click Update to save your changes.

Security Users

Security users or clients are authorized to receive notifications (traps or informs) sent to the
RealPresence DMA system.

Add a Security User

For SNMPv3 notifications, you must specify at least one security user.

Procedure

1. Go to Admin > Server > SNMP Settings.
2. Under Security User, click the add button.
3. In the Add Security User window, configure the settings described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication protocol used to create unique fixed-sized message digests of a variable length message.</td>
</tr>
<tr>
<td></td>
<td>▪ MD5 - Creates a digest of 128 bits (16 bytes)</td>
</tr>
<tr>
<td></td>
<td>▪ SHA - Creates a digest of 160 bits (20 bytes)</td>
</tr>
<tr>
<td></td>
<td>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB).</td>
</tr>
<tr>
<td>Authentication password</td>
<td>The authentication password that is used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Encryption type</td>
<td>The privacy protocol for the connection between the RealPresence DMA system and the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>▪ DES - Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td></td>
<td>▪ AES - Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td>Encryption password</td>
<td>The password that the privacy protocol uses, together with the local engine ID, to create the encryption key.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

4. Click OK.
   The user displays in the Security User list.
5. Click Update to save the settings.
Edit a Security User

The settings for a security user can be revised as needed.

Procedure
1. Go to Admin > Server > SNMP Settings.
2. From the Security User list, select the user to edit.
3. Click the edit button.
4. Revise the following settings in the Edit Security User window as needed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
<tr>
<td>Authentication type</td>
<td>The authentication protocol used to create unique fixed-sized message digests of a variable length message.</td>
</tr>
<tr>
<td></td>
<td>- MD5 - Creates a digest of 128 bits (16 bytes)</td>
</tr>
<tr>
<td></td>
<td>- SHA - Creates a digest of 160 bits (20 bytes)</td>
</tr>
<tr>
<td></td>
<td>Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.</td>
</tr>
<tr>
<td></td>
<td>The RealPresence DMA system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB).</td>
</tr>
<tr>
<td>Authentication password</td>
<td>The authentication password that is used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
<tr>
<td>Encryption type</td>
<td>The privacy protocol for the connection between the RealPresence DMA system and the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>- DES - Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td></td>
<td>- AES - Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td>Encryption password</td>
<td>The password that the privacy protocol uses, together with the local engine ID, to create the encryption key.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>

5. Click OK.
6. Click Update to save the settings.

Delete a Security User

Delete security users when you no longer want them to receive SNMP notifications.

Procedure
1. Go to Admin > Server > SNMP Settings.
2. In the Security User list, select the user to delete.
3. Click the delete button.
4. Click Yes to confirm the deletion.
5. Click **Update** to save your changes.

**Download MIBs**

The following MIBs are available from the RealPresence DMA system.

You can download any of them from the **SNMP Settings** page.

Polycom recommends that you view MIB files with a MIB viewer application.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB-Dell-10892</td>
<td>The hardware-specific MIB.</td>
</tr>
<tr>
<td>POLYCOM-BASE-MIB</td>
<td>The base MIB for Polycom products.</td>
</tr>
<tr>
<td>POLYCOM-DMA-MIB</td>
<td>The RealPresence DMA system-specific MIB definition.</td>
</tr>
<tr>
<td>POLYCOM-MCU-MANAGEMENT</td>
<td>The Polycom MCU MIB that contains MCU-related information, including MCU states.</td>
</tr>
<tr>
<td>RFC1213-MIB</td>
<td>The MIB for TCP/IP network management.</td>
</tr>
<tr>
<td>SNMPv2-CONF</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-SMI</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-TC</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Go to **Admin > Server > SNMP Settings**.
2. Click **Download MIBs**.
3. Select the MIB to download.
4. Click **Download**.
5. Save or open the MIB file locally.
6. Click **OK** to close the **Download DMA MIBS** window.
Reports

Topics:

- Alert History
- Call History
- Conference History
- Registration History
- Call Detail Records
- Network Usage Report

This section provides an introduction to using and configuring Polycom RealPresence DMA system reports.
Alert History

You can view all the system alerts for the time period you select.
The system retains the most recent 500 alerts. Each alert includes the start and end time, alert code, and description.

Procedure

1. Go to Reports > Alert History.
2. Use the search section above the list as follows to find alerts matching the criteria you specify:
   - Click the filter icon to expand the search section.
   - Select the appropriate filter to search by description, alert code, or time period.
3. Click Search to display the results.
Call History

Topics:

- Search Call History
- Export Search Results
- Show Export History
- Hide Export History
- Show Call Details

You can view detailed records of calls and download call detail records (CDRs). The records include point-to-point calls through the call server and VMR calls through the conference manager.

RealPresence DMA core systems also display the call history of an integrated edge system (or other core system in a VPN tunnel) that didn't have call licenses. However, not all call details display on the core system. To see complete call details, view them from the edge or other core system.

Related Links
- Search Call History on page 549
- View Call History on page 530

Search Call History

You can view call history in a RealPresence DMA system and use filters to search for call records.

You can search for calls by dial string and limit the results by specifying one or more of the following:

- Originator device’s name, alias, or IP address
- Destination device’s name, alias, or IP address
- Signaling type used in the call (H.323, SIP, WebRTC)
- Registration status of the call originator
- Cluster, territory, or site

Procedure

1. Go to Reports > Call History.
2. Use the search pane above the list as follows to find calls matching the criteria you specify:
   - Select the filter button to expand the search pane.
   - Select the appropriate filters to narrow your search results.
3. Select Search to display the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator</td>
<td>The originating device’s display name, name, alias, or IP address (in that</td>
</tr>
<tr>
<td></td>
<td>order of preference), depending on what it provided in the call signaling.</td>
</tr>
<tr>
<td></td>
<td>If the originator is an MCU, the MCU name.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial string</td>
<td>Dial string sent by originator, when available.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is an MCU, the MCU name; if a VSC, the VSC value (not including the VSC).</td>
</tr>
<tr>
<td>Start time</td>
<td>Time the call began (first signaling event).</td>
</tr>
<tr>
<td>End time</td>
<td>Time the call ended (session closed).</td>
</tr>
<tr>
<td>Ingress cluster</td>
<td>The cluster (the first, if more than one) that handled the call.</td>
</tr>
<tr>
<td>Call ID</td>
<td>Unique identifier for the call.</td>
</tr>
</tbody>
</table>

### Related Links

[Call History on page 549](#)

### Export Search Results

The **Export Search Results** command lets you download just the records displayed on the page (the current search results).

A **Save** dialog prompts you to select a location for the downloaded file. The default filename is **CDRSearchExport.tar**. This is a troubleshooting feature. To aid in resolving a problem, Polycom Global Services may ask you to use specific search criteria to retrieve certain call records, download the records, and send the file to them for analysis.

### Show Export History

The **Export History** list provides a record of the CDR exports and search results exported from the system.

The list includes the following fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID of the person who performed the export.</td>
</tr>
<tr>
<td>Export type</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">CDR</a> for CDR exports</td>
</tr>
<tr>
<td></td>
<td>• <a href="#">Call History</a> for search results exports</td>
</tr>
<tr>
<td>Date of export</td>
<td>Date and time of the export.</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster from which the export took place.</td>
</tr>
</tbody>
</table>
The Export History list is the same on the Call History and Conference History pages. In both places, all export operations are shown.

Procedure
1. Go to Reports > Call History or Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History.
   The Export History list displays below the list of search results.

Hide Export History
You can hide the Export History list from the Call History or Conference History page when necessary.

Procedure
1. Go to Reports > Call History or > Conference History.
2. Search for calls or conferences based on the criteria you need to match.
3. Under Actions, click Show Export History.
   The Export History list displays below the list of search results.
4. When you finish viewing the Export History, click Hide Export History.

Show Call Details
Call details provide specific information about any call you select from the list of calls.

Procedure
1. Go to Reports > Call History.
2. Search for calls based on the criteria you need to match.
3. Select a call from the list of search results and click Show Call Details.
   The Call Details window displays.
4. Select from the categories on the left side of the window to display related details.
Conference History

Topics:

- Show Export History
- Hide Export History
- Associated Calls
- Conference Events
- Property Changes

The Conference History page lets you view detailed records of conferences and download call detail records (CDRs).

The fields at the top of the page let you specify the starting and ending date and time or the conference ID for which you want to view conference records.

When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

After you search for conferences, the Conference History page lists all the conferences in the time range you specified. If there are more than 500, the first page lists the first 500, and the arrow buttons below the list let you view other pages. The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference room ID</td>
<td>The conference room ID.</td>
</tr>
<tr>
<td>Start time</td>
<td>Time the conference began (first conference event).</td>
</tr>
<tr>
<td>End time</td>
<td>Time the conference ended (last conference event).</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster that handled the conference.</td>
</tr>
</tbody>
</table>

Show Export History

The Export History list provides a record of the CDR exports and search results exported from the system.

The list includes the following fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID of the person who performed the export.</td>
</tr>
<tr>
<td>Export type</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>- CDR for CDR exports</td>
</tr>
<tr>
<td></td>
<td>- Call History for search results exports</td>
</tr>
</tbody>
</table>
**Export History** list is the same on the **Call History** and **Conference History** pages. In both places, all export operations are shown.

**Procedure**
1. Go to **Reports > Call History** or **Conference History**.
2. Search for calls or conferences based on the criteria you need to match.
3. Under **Actions**, click **Show Export History**.
   - The **Export History** list displays below the list of search results.

**Hide Export History**
You can hide the **Export History** list from the **Call History** or **Conference History** page when necessary.

**Procedure**
1. Go to **Reports > Call History** or **Conference History**.
2. Search for calls or conferences based on the criteria you need to match.
3. Under **Actions**, click **Show Export History**.
   - The **Export History** list displays below the list of search results.
4. When you finish viewing the **Export History**, click **Hide Export History**.

**Associated Calls**
The **Associated Calls** list shows all the calls associated with the selected conference.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call ID</td>
<td>Unique identifier for the call.</td>
</tr>
<tr>
<td>Start time</td>
<td>Time the call began (first signaling event).</td>
</tr>
<tr>
<td>End time</td>
<td>Time the call ended (session closed).</td>
</tr>
<tr>
<td>Originator</td>
<td>The originating device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is an MCU, the MCU name; if a VSC, the VSC value (not including the VSC).</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Cluster</td>
<td>The cluster (first, if more than one) that handled the call.</td>
</tr>
</tbody>
</table>

The **Display Call History** command (in the **Actions** list) takes you to the **Call History** page and displays the call that was selected in the **Associated Calls** list.

## Conference Events

The **Conference Events** list provides much more detail about the selected conference, listing every state change and call event in the course of the conference.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Information about the event (varies with the event type).</td>
</tr>
<tr>
<td>Call UUID</td>
<td>Call identifier (if call event).</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of the event.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Identifies when in the order of changes to this conference this event occurred.</td>
</tr>
</tbody>
</table>

When you select a conference event with a call UUID, the **Display Call History** command (in the **Actions** list) takes you to the **Call History** page and displays the associated call.

## Property Changes

The **Property Changes** list provides more information about the selected conference, listing every change in the value of a conference property during the conference.

The following table describes the fields in the list.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the call property.</td>
</tr>
<tr>
<td>Value</td>
<td>Value assigned to the property.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time of the property change.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Identifies when in the order of changes to this call this property change occurred.</td>
</tr>
</tbody>
</table>
Registration History

Topics:

- View the Registration History

Registration History provides access to information about registered devices. It also provides information about external SIP peers with which the system is registered, if any.

View the Registration History

When the call server is providing H.323 gatekeeper or SIP registrar services, you can view information about registered devices.

Procedure

1. Go to Reports > Registration History.

   The following fields display in the registrations list:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the registered device.</td>
</tr>
<tr>
<td>Alias</td>
<td>The device's alias.</td>
</tr>
<tr>
<td>Start time</td>
<td>The time and date that the device registered.</td>
</tr>
<tr>
<td>End time</td>
<td>The time and date that the device's registration ended (blank if the device is still registered).</td>
</tr>
<tr>
<td>Registration status</td>
<td>The registration status:</td>
</tr>
<tr>
<td></td>
<td>- Active</td>
</tr>
<tr>
<td></td>
<td>- Rejected</td>
</tr>
<tr>
<td></td>
<td>- Terminated by call server</td>
</tr>
<tr>
<td></td>
<td>- Terminated by endpoint</td>
</tr>
<tr>
<td></td>
<td>- Timed out</td>
</tr>
</tbody>
</table>

2. Use the search section above the list as follows to find registrations matching the criteria you specify:

   - Click the filter icon to expand the search section.
   - Select the appropriate filter to search by alias or IP address.

3. Limit your search as needed by specifying one or more of the following:

   - Owner, territory, or site
   - Signaling protocol (H.323 or SIP)
   - Registration status
4. Click **Search**.
   
The registrations that match your search criteria display below the search fields.

5. Under **Actions**, click **Show Details** to display the **Registration Details** and the **Events and Signaling Messages** tabs below the list, enabling you to see:
   
   ▪ Detailed information about the selected device's registration status and information.
   
   ▪ A history of the registration signaling and processing, including the results of applying the registration policy script, if any (see Registration Policy).
Call Detail Records

Topics:

- Export CDR Data

The RealPresence DMA system generates call detail records (CDRs) for all calls and conferences, which you can download.

After you unzip the download file, you can open the two CSV files it contains (one for calls and one for conferences) with a spreadsheet application. The CSV files contain a line for each call or conference that ended during the selected time frame.

The ZIP file also includes a text file that contains a single line specifying:

- The number of calls in the call CDR file.
- The number conferences in the conference CDR file.
- The clusters whose calls and conferences are included in the CDR file.
- The clusters whose calls and conferences are excluded from the CDR file because those clusters were not reachable when the CDR export was generated.

**Caution:** Only one CDR should be generated at a time. If you run a client application that issues API calls to automatically generate and download CDRs at the same time that you manually attempt to generate and download a CDR, you or the client application may receive errors.

**Export CDR Data**

From the Call History or Conference History page, you can download call detail records for the time period you specify.

Note the following:

You can't create multiple CDR queries from the Call History page.

When you run a CDR query, the status of the query displays.

If a previous CDR query exists, you can download the results of the query.

**Procedure**

1. Go to Reports > Call History or Conference History.
2. Select Export CDR Data.
3. In the Export Time Frame dialog, set the Calls and conferences ending after date and time and the Calls and conferences ending before date and time as the parameters for your CDR data query.
   
   The defaults provide all CDR data for the current day. Times and dates are in the time zone of your browser.
4. Click OK.
   
   The system displays the progress as it gathers the information needed to construct the CDR data files.
5. When the **Exporting CDR Data** dialog displays **Data has been prepared and is ready to be downloaded**, click **Download** to select a location for the downloaded file.

6. Choose a path and filename for the CDR file and click **Save**.

   The **Exporting CDR Data** dialog shows the progress.

7. When the download is complete, click **Close**.

**Call Record Layouts**

Call detail records (CDRs) contain information about calls that occurred in the time frame you specify.

Field values are enclosed in double quotes in these situations:

- They begin or end with a space or tab (" value").
- They contain a comma ("Smith, John").
- They contain a double quote. In that case, each double quote is also preceded by a double quote ("William ""Bill"" Smith").

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Changes each time the format of CDRs changes.</td>
</tr>
<tr>
<td>type</td>
<td>CALL</td>
</tr>
<tr>
<td>callType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>▪ PT-PT</td>
</tr>
<tr>
<td></td>
<td>▪ VMR</td>
</tr>
<tr>
<td></td>
<td>▪ VEQ</td>
</tr>
<tr>
<td></td>
<td>▪ VSC-hunt group</td>
</tr>
<tr>
<td></td>
<td>▪ VSC-[uncond fwd</td>
</tr>
<tr>
<td></td>
<td>▪ VMR-subscribe only</td>
</tr>
<tr>
<td></td>
<td>▪ VMR-Lync AVMCU</td>
</tr>
</tbody>
</table>

**Note:** For Polycom and Cisco Immersive Telepresence (ITP) rooms using Cisco TIP signaling, all the codecs (endpoint devices in the room) signal using a single session, producing a single CDR. For Polycom ITP systems using SIP signaling (but not H.323), if the codecs follow the prescribed naming convention (see Naming ITP Systems Properly for Recognition by the RealPresence DMA system), the RealPresence DMA system recognizes them as constituting a single ITP system and creates a single CDR for the ITP system rather than separate CDRs for each of its codecs: The first three fields in the CDR (version, type, callType) contain a single value associated with the primary (sequence number 1) codec. The remaining fields contain an escaped (quote-enclosed) comma-separated list of values, one for each codec in the ITP system.

Times and dates in the CDR file are expressed in the time zone of the RealPresence DMA system that created the CDR export, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for `endTime` will be different from the offset for `startTime`.

The following table describes the fields in the call detail records. Note that some fields have been deprecated. These fields will be listed in CDRs but will not report any data.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callUuid</td>
<td>Unique identifier for the call.</td>
</tr>
<tr>
<td>dialin</td>
<td>If this is point-to-point or a VMR dial-in call, TRUE. Otherwise, FALSE.</td>
</tr>
<tr>
<td>startTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>This is when call signaling reached the RealPresence DMA system, not when media started. If multiple call records, the start of this segment of the call.</td>
</tr>
<tr>
<td>endTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td></td>
<td>This is when the RealPresence DMA system’s involvement with the call ended, not when media ended. If multiple call records, the end of this segment of the call.</td>
</tr>
<tr>
<td>origEndpoint</td>
<td>The originating endpoint's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the originator is an MCU, the MCU name.</td>
</tr>
<tr>
<td>dialString</td>
<td>Initial dial string as supplied by the originator. If multiple call records, this value is the same across all segments of the call.</td>
</tr>
<tr>
<td>destEndpoint</td>
<td>The destination endpoint's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is an MCU, the MCU name; if a VSC, the VSC value (not including the VSC character).</td>
</tr>
<tr>
<td>origSignalType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• h323</td>
</tr>
<tr>
<td></td>
<td>• sip</td>
</tr>
<tr>
<td>destSignalType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• h323</td>
</tr>
<tr>
<td></td>
<td>• sip</td>
</tr>
<tr>
<td>refConfUUID</td>
<td>If VMR call, confUUID of the associated conference.</td>
</tr>
<tr>
<td>lastForwardEndpoint</td>
<td>If call forwarding, endpoint that forwarded call to the final destination endpoint.</td>
</tr>
<tr>
<td>cause</td>
<td>Cause value for call termination or termination of this CDR. This may not be the end of the call.</td>
</tr>
<tr>
<td>causeSource</td>
<td>Source of the termination of the call record. Indicates which participant requested call disconnect:</td>
</tr>
<tr>
<td></td>
<td>• originator</td>
</tr>
<tr>
<td></td>
<td>• destination</td>
</tr>
<tr>
<td></td>
<td>• callserver</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bitRate</td>
<td>Bit rate for call, in kbps. If the bit rate changes during the call, this is a list of bit rate values separated by plus signs (+). For instance: 1024+768+384</td>
</tr>
<tr>
<td>classOfService</td>
<td>Class of service for the call:</td>
</tr>
<tr>
<td></td>
<td>• Gold</td>
</tr>
<tr>
<td></td>
<td>• Silver</td>
</tr>
<tr>
<td></td>
<td>• Bronze</td>
</tr>
<tr>
<td>ingressCluster</td>
<td>The RealPresence DMA cluster of the originating endpoint or entry point from a neighbor or SBC.</td>
</tr>
<tr>
<td>egressCluster</td>
<td>The RealPresence DMA cluster of the destination endpoint or exit point to a neighbor or SBC.</td>
</tr>
<tr>
<td>VMRCluster</td>
<td>The RealPresence DMA cluster handling the VMR, or blank if not a VMR call.</td>
</tr>
<tr>
<td>VEQCluster</td>
<td>The RealPresence DMA cluster handling the VEQ, or blank if no VEQ.</td>
</tr>
<tr>
<td>userRole</td>
<td>If VMR call, the role of the caller in conference:</td>
</tr>
<tr>
<td></td>
<td>• PARTICIPANT</td>
</tr>
<tr>
<td></td>
<td>• CHAIRPERSON (entered passcode)</td>
</tr>
<tr>
<td></td>
<td>Null if not VMR call.</td>
</tr>
<tr>
<td>userDataA</td>
<td>The value from the User pass-through to CDR field of the user associated with the endpoint that started this call.</td>
</tr>
<tr>
<td>userDataB</td>
<td>For VMR calls, the value from the Conference room pass-through to CDR field of the conference room (VMR) to which the call connected.</td>
</tr>
<tr>
<td></td>
<td>For point-to-point calls, the value from the User pass-through to CDR field of the user associated with the endpoint that received this call.</td>
</tr>
<tr>
<td>userDataC</td>
<td>For VMR calls, the dial-out participant pass-through value provided via the API, if any.</td>
</tr>
<tr>
<td></td>
<td>For point-to-point calls, not currently used.</td>
</tr>
<tr>
<td>userDataD</td>
<td>Not currently used.</td>
</tr>
<tr>
<td>userDataE</td>
<td>Not currently used.</td>
</tr>
<tr>
<td>failureSignalingCode</td>
<td>For SIP calls, the SIP code and reason, separated by a colon, that the call was disconnected. For instance: 486:BUSY HERE</td>
</tr>
<tr>
<td>origModel</td>
<td>The hardware model of the originating device, if available from the device’s registration or other signaling.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>origVersion</td>
<td>The software version of the originating device, if available from the device's registration or other signaling.</td>
</tr>
<tr>
<td>destModel</td>
<td>The hardware model of the destination device, if available from the device's registration or other signaling.</td>
</tr>
<tr>
<td>destVersion</td>
<td>The software version of the destination device, if available from the device's registration or other signaling.</td>
</tr>
<tr>
<td>displays</td>
<td>For an immersive telepresence room, the number of screens the room has. For a Polycom SIP ITP call, this is determined from the system name; for a Polycom or Cisco TIP call, it's the <strong>x-cisco-multiple-screen</strong> parameter value. For all other calls, the value is 1. <strong>Note:</strong> If a Polycom ITP room doesn't follow the ITP naming convention, this field may contain inaccurate information.</td>
</tr>
<tr>
<td>minVideoResolution</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>maxVideoResolution</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>videoPeakJitter</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>videoTotalPackets</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>videoTotalLostPackets</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>minContentResolution</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>maxContentResolution</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>contentPeakJitter</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>contentTotalPackets</td>
<td>Deprecated – blank</td>
</tr>
<tr>
<td>contentTotalLostPackets</td>
<td>The number of packets lost on the content channel. Zero (0) if content was not shared. Available only for AVC calls using SIP or TIP signaling to a version 8.1 or newer hardware-based Polycom MCU with MPMx cards. Otherwise, blank.</td>
</tr>
<tr>
<td>origSignalingId</td>
<td>For SIP point-to-point or VMR calls (dialin=TRUE), the complete From header of the INVITE received from the endpoint. For VMR SIP dial-outs (dialin=FALSE), the To header sent by the RealPresence DMA system to the MCU. Otherwise, blank.</td>
</tr>
<tr>
<td>origCallId</td>
<td>The SIP or H.323 call ID of the call between the originating endpoint and the RealPresence DMA system. For VMR dial-outs, the call ID of the call between the RealPresence DMA system and the MCU.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>destCallId</td>
<td>The SIP or H.323 call ID of the call between the destination endpoint and the RealPresence DMA system. For calls to a VMR, the call ID of the call between the RealPresence DMA system and the MCU.</td>
</tr>
<tr>
<td>chairPasscode</td>
<td>The configured chairperson passcode for the conference room. Blank if no passcode was configured at the time of the conference.</td>
</tr>
<tr>
<td>confRequiresChair</td>
<td>TRUE if the conference template used for the conference has the Conference requires chairperson flag enabled. Otherwise, FALSE.</td>
</tr>
<tr>
<td>termConfAfterChairDrops</td>
<td>TRUE if the conference template used for the conference has the Terminate conference after chairperson drops flag enabled. Otherwise, FALSE.</td>
</tr>
<tr>
<td>charJoinTime</td>
<td>The time the first chairperson joined the conference. If no chairperson joined the conference, blank.</td>
</tr>
</tbody>
</table>

**Conference Record Layouts**

Call Detail Records (CDRs) contain information about conferences that occurred in the time frame you specify.

Field values are enclosed in double quotes in these situations:

- They begin or end with a space or tab (" value").
- They contain a comma ("Smith, John").
- They contain a double quote. In that case each double quote is also preceded by a double quote ("William ""Bill"" Smith").

Times and dates in the CDR file are expressed in the time zone of the RealPresence DMA cluster that created the CDR export, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for endTime will be different from the offset for startTime.

The following table describes the fields in the conference records.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>Changes each time the format of CDRs changes.</td>
</tr>
<tr>
<td>type</td>
<td>CONF</td>
</tr>
<tr>
<td>confType</td>
<td>One of the following:</td>
</tr>
<tr>
<td></td>
<td>• PCO - for Polycom Conferencing for Outlook (calendared) conferences</td>
</tr>
<tr>
<td></td>
<td>• LYNC - for Lync conferences</td>
</tr>
<tr>
<td></td>
<td>• AD-HOC - for all other conferences</td>
</tr>
<tr>
<td>cluster</td>
<td>The RealPresence DMA cluster serving the VMR.</td>
</tr>
<tr>
<td>confUUID</td>
<td>Unique identifier for the conference.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>startTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
<tr>
<td>endTime</td>
<td>YYYY-MM-DDTHH:MM:SS.FFF[+</td>
</tr>
</tbody>
</table>
| userID    | Conference room (VMR) owner, shown as: domain\user  
Domain is LOCAL for non-AD users.  
If this is a Lync conference, this field is empty.                                                                                                           |
| roomID    | Conference room (VMR) number or Lync conference ID.                                                                                                                                                           |
| partCount | Maximum number of concurrent calls in the conference (high water mark).  
Doesn't include audio-only IVR dial-outs or participants dialed directly into or out from the MCU without going through the RealPresence DMA system.  
The following are counted as a single participant:  
▪ A Polycom or Cisco immersive telepresence room using Cisco TIP signaling.  
▪ A Polycom ITP room using SIP signaling and the prescribed naming convention. (see Naming ITP Systems Properly for Recognition by the Polycom RealPresence DMA System). |
| classOfService | Class of service for the call:  
▪ Gold  
▪ Silver  
▪ Bronze                                                                                                           |
<p>| userDataA | The value from the <strong>User pass-through to CDR</strong> field of the user associated with the conference room (VMR).                                                                                                      |
| userDataB | The value from the <strong>Conference room pass-through to CDR</strong> field of the conference room (VMR).                                                                                                                                 |
| userDataC | The conference ID provided via the API, if any.                                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| maxResourcesUsed      | The maximum number of video and voice ports used for the conference, reported as follows:  
video: <video port count>  
voice: <voice port count>  
Available only for conferences on a RealPresence Collaboration Server or RMX MCU that provides this information.  
**Note:** Voice calls may use video ports if voice ports aren't available.  
**Note:** The RealPresence DMA system reports port numbers based on resource usage for CIF calls. Version 8.1 and later Polycom MCUs report port numbers based on resource usage for HD720p30 calls. In general, 3 CIF = 1 HD720p30, but it varies depending on bridge/card type and other factors.  
See your Polycom RealPresence Collaboration Server or RMX system documentation for more detailed information about resource usage. |
| mcuNameList           | The MCUs used by the conference. If there is more than one (due to cascading or an MCU failover), this is a comma-separated list enclosed in quotes.  
If the conference was cascaded, the hub MCU is listed first. If there was a failover, the original MCU is listed first.                                                                                           |
| confDisplayNameList   | The conference display name of the conference as it appears on the MCU. If there is more than one MCU (due to cascading or an MCU failover), this is a comma-separated list enclosed in quotes.  
If the conference was cascaded, the display name from the hub MCU is listed first. If there was a failover, the display name from the original MCU is listed first.  
This information is included to support the correlation of RealPresence DMA CDRs with CDRs on the MCU. Polycom MCUs use the conference display name as part of the name of the CDR file for a conference. |
| chairPasscode         | The configured chairperson passcode for the conference room. Blank if no passcode was configured at the time of the conference.                                                                                                                                                  |
| confRequiresChair     | TRUE if the conference template used for the conference has the **Conference requires chairperson** check box enabled. Otherwise, FALSE.                                                                                                                                               |
| termConfAfterChairDrops| TRUE if the conference template used for the conference has the **Terminate conference after chairperson drops** check box enabled. Otherwise, FALSE.                                                                                                                             |
| charJoinTime          | The time that the first chairperson joined the conference. If no chairperson joined the conference, blank.                                                                                                                                                                    |
Network Usage Report

Topics:

- Export Network Usage Data
- View Network Usage Data

The Network Usage page displays historical usage data about the video network. You can export the network usage data as a CSV (comma-separated values) file. Use the search feature to select the network usage criteria to include in the report:

- Start time and span/granularity data
- Cluster, territory, or throttlepoint (site, site link, or subnet) data
- Specific call, QoS, and bandwidth data

The data matching the criteria you choose displays as a graph.

Export Network Usage Data

You can download a comma-separated values (CSV) file that contains all the network usage data point records for the time period you specify.

A network usage data report contains records only for a single cluster (one or two RealPresence DMA systems) or a HA pair, not for all superclustered systems.

The system retains the most recent 8 million data points.

Procedure

1. Go to Monitoring > Network Usage.
2. Enter the following search criteria as needed:
   - Time granularities
   - Start time
   - Type
   - Value
3. Click Search to display specific call, QoS, and bandwidth data you want to see.
4. Click Export Network Usage.
5. Set the Export Time Frame Start Date and time and the Export Time Frame End Date and time you want to include.

   The default values provide all network usage data for the past 24 hours.
6. Click OK.
7. Choose a path and filename for the network usage file and click Save.
8. When the download is complete, click Close.

   You can open the CSV file with Microsoft Excel or another spreadsheet application.
View Network Usage Data

When you export network usage data, the file includes a network usage data point record for each throttlepoint, territory, and cluster for each minute of the time period you specified for the report.

It doesn’t include usage data for MPLS clouds, the default Internet site, or sites not controlled by the system.

The following table describes the fields in the records.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of the throttlepoint, territory, or cluster that defines the scope being measured.</td>
</tr>
<tr>
<td>date</td>
<td>Minutes since 1970 (Java time / 60,000).</td>
</tr>
<tr>
<td>calls_started</td>
<td>Number of calls started in the scope during the time interval.</td>
</tr>
<tr>
<td>calls Ended</td>
<td>Number of calls ended in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_dropped</td>
<td>Number of calls rejected or evicted due to bandwidth limits at the throttlepoint during the time interval. The calls dropped measure is intended to help with understanding network congestion. So, it includes calls dropped due to available bandwidth at the throttlepoint, but not calls dropped due to per call bit rate limits at the throttlepoint.</td>
</tr>
<tr>
<td>calls_downspeeded</td>
<td>Number of calls downspeeded due to bandwidth limits at the throttlepoint during the time interval. The calls downspeeded measure is intended to help with understanding network congestion. So, it includes calls downspeeded due to available bandwidth at the throttlepoint, but not calls downspeeded due to per call bit rate limits at the throttlepoint.</td>
</tr>
<tr>
<td>bitrate_limit</td>
<td>The (maximum) configured bit rate limit for the scope during the time interval, or -1 if no limit was configured (kbps).</td>
</tr>
<tr>
<td>bandwidth_limit</td>
<td>The (maximum) configured bandwidth limit for the scope during the time interval, or -1 if no limit was configured (kbps).</td>
</tr>
<tr>
<td>bandwidth_usage</td>
<td>The (maximum) used bandwidth for the scope during the time interval (kbps).</td>
</tr>
<tr>
<td>bandwidth_usage_percent</td>
<td>The (maximum) percentage of the bandwidth limit used for the scope during the time interval (kbps).</td>
</tr>
<tr>
<td>packet_loss_percent</td>
<td>Mean packet loss percentage of all QoS reports in the scope during the time interval.</td>
</tr>
<tr>
<td>avg_video_jitter</td>
<td>Mean jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_video_jitter</td>
<td>Maximum jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_video_delay</td>
<td>Mean delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>max_video_delay</td>
<td>Maximum delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_audio_jitter</td>
<td>Mean jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_audio_jitter</td>
<td>Maximum jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>avg_audio_delay</td>
<td>Mean delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>max_audio_delay</td>
<td>Maximum delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).</td>
</tr>
<tr>
<td>gold_calls</td>
<td>Max concurrent Gold class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>silver_calls</td>
<td>Max concurrent Silver class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>bronze_calls</td>
<td>Max concurrent Bronze class calls in the scope during the time interval.</td>
</tr>
<tr>
<td>audio_calls</td>
<td>Max concurrent audio calls in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_256Kbps</td>
<td>Max concurrent video calls with a bit rate less than or equal to 320 kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_384Kbps</td>
<td>Max concurrent video calls with a bit rate greater than 320 kbps and less than or equal to 448 kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_512Kbps</td>
<td>Max concurrent video calls with a bit rate greater than 448 kbps and less than or equal to 640 kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_768Kbps</td>
<td>Max concurrent video calls with a bit rate greater than 640 kbps and less than or equal to 896 kbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_1Mbps</td>
<td>Max concurrent video calls with a bit rate greater than 896 kbps and less than or equal to 1.5 Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_2Mbps</td>
<td>Max concurrent video calls with a bit rate greater than 1.5 Mbps and less than or equal to 3 Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>calls_4Mbps</td>
<td>Max concurrent video calls with a bit rate greater than 3 Mbps in the scope during the time interval.</td>
</tr>
<tr>
<td>sip_calls</td>
<td>Max concurrent calls using SIP signaling in the scope during the time interval.</td>
</tr>
<tr>
<td>h323_calls</td>
<td>Max concurrent calls using H.323 signaling in the scope during the time interval.</td>
</tr>
<tr>
<td>gateway_calls</td>
<td>Max concurrent calls using the SIP to H.323 gateway in the scope during the time interval.</td>
</tr>
<tr>
<td>conference_calls</td>
<td>Max concurrent conference manager calls in the scope during the time interval.</td>
</tr>
</tbody>
</table>
Troubleshooting

Topics:

- Alerts
- Troubleshooting Utilities
- RealPresence DMA System Network Configurations

This section provides an introduction to troubleshooting in the Polycom RealPresence DMA system.
Alerts

Topics:

- Supercluster Status
- Territory Status
- RealPresence Resource Manager System Integration
- Active Directory Integration
- Exchange Server Integration
- Database Status
- Skype for Business Integration
- Signaling
- Certificate
- Licenses
- Networks
- Server Resources
- Data Synchronization
- System Health and Availability
- Cluster Features
- MCUs
- Endpoints
- Conference Manager
- Conference Status
- Skype for Business Presence Publishing
- Call Server
- Call Bandwidth Management

On various pages and the dashboard section, the alert icon indicates that an abnormal condition, problem, or something you should be aware of.

Hover over the icon to see details.

A summary of alert status appears in the menu bar, showing how many alerts exist across all clusters of a supercluster and how many are new (not viewed yet).

When you click the summary data, an expanded alerts list appears, displaying the date and time, alert code, and description of each alert. In many cases, the alert description is a link to the relevant page. A Help button displays the help topic for that alert, and contains additional information and recommendations for the alert.

The following topics describe the alerts by category, followed by the alerts contained in the category:
Supercluster Status

The following alerts provide information on changes in cluster and supercluster status.

**Alert 1001**

You or another administrator busied out the cluster, perhaps for maintenance.

A busied-out cluster allows existing calls and conferences to continue and accepts new calls for existing conferences, but does not accept other new calls and conferences.

Once all existing calls and conferences have ended, the cluster is out of service.

Click the link to go to the DMAs page.

**Alert 1002**

You or another administrator took the cluster out of service (or busied out the cluster, and now all calls and conferences have ended).

*Cluster <cluster> is out of service as of YYYY-MM-DD HH:MM GMT+/-H[:MM]*.

An out-of-service cluster is still running and accessible via the management interface, but does not accept any calls or registrations.

Click the link to go to the DMAs page.

**Alert 1003**

The replication link with the specified cluster seems to be corrupted.

*Cluster <cluster> is orphaned.*

Click the link to go to the DMAs page. Try removing that cluster from the supercluster and then rejoining.

**Alert 1004**

The specified cluster is not sending scheduled heartbeats.

*Cluster <cluster> is not reachable. Last heartbeat received YYYY-MM-DD HH:MM GMT+/-H[:MM].*

Possible reasons include:

- The cluster may simply be very busy and have fallen behind in sending heartbeats.
- An internal process could be stuck.
- The servers may be offline or rebooting.
- There may be a network problem.

Click the link to go to the DMAs page.

Territory Status

The following alerts provide information on changes in territory status.
Alert 1103
The specified territory or territories are not assigned to a cluster, so any responsibilities assigned to the territories are not being fulfilled.

No clusters assigned to <list of territories>.
Click the link to go to the Territories page. Assign a primary and backup cluster for every territory in your site topology.

Alert 1105
The cluster from which the alert originated is unable to communicate with the specified territory's primary and backup clusters.

>alerting-cluster>: Primary cluster <p-cluster> and backup cluster <b-cluster> are not reachable. Territory <territory> may not be functioning.
This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the clusters in question.
If this alert reoccurs frequently but quickly goes away, that suggests intermittent spurious network problems. If it persists for more than about 15-30 seconds, it may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).
Click the link to go to the Territories page. To enable conferencing to continue in the territory (at diminished capacity), assign it to some other cluster.

Alert 1106
The cluster from which the alert originated is unable to communicate with the specified territory's primary cluster, and there is no backup cluster.

>alerting-cluster>: Cluster <cluster> is not reachable. Territory <territory> may not be functioning.
This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the cluster in question.
If this alert reoccurs frequently but quickly goes away, that suggests intermittent spurious network problems. If it persists for more than about 15-30 seconds, it may indicate serious network problems. It is also possible that someone shut the cluster down or that it failed.
Click the link to go to the Territories page. To enable conferencing to continue in the territory (at diminished capacity), assign it to some other cluster.
We recommend assigning a backup cluster for each territory.

Alert 1107
The cluster from which the alert originated is unable to communicate with the specified territory's primary cluster, but can communicate with the backup cluster.

>alerting-cluster>: Primary cluster <p-cluster> associated with territory <territory> is not reachable. But backup cluster <b-cluster> is reachable.
This may be a temporary problem, in which case this alert will be cleared as soon as the alerting cluster is once again able to communicate with the cluster in question.
If this alert reoccurs frequently but quickly goes away, that suggests intermittent network problems. If it persists, it will be followed by alert 1108, indicating that the territory has failed over to the backup cluster. The backup cluster allows conferencing to continue in the territory (at diminished capacity) and fulfills any other responsibilities assigned to the territory.

Click the link to go to the Territories page. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster's IP addresses.

If this is a two-server cluster, and you cannot ping either the virtual or physical IP addresses, look for a network problem. It is unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the servers.

**Alert 1108**

The territory's primary cluster is unreachable, and its backup cluster has taken over.

<alerting-cluster>: Territory <territory> has failed over from <p-cluster> to <b-cluster>.

This may indicate a network problem. It is also possible that someone shut the cluster down or that it failed.

The backup cluster allows conferencing to continue in the territory (at diminished capacity) and fulfills any other responsibilities assigned to the territory.

Click the link to go to the Territories page. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster's IP addresses.

If this is a two-server cluster, and you can't ping either the virtual or physical IP addresses, look for a network problem. It's unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the servers.

**RealPresence Resource Manager System Integration**

The following alerts provide information on RealPresence Resource Manager system integration events and changes in integration status.

**Alert 2001**

An error occurred when the cluster responsible for RealPresence Resource Manager integration tried to synchronize data with the RealPresence Resource Manager system.

<formatted string from server>

The alert text describes the nature of the problem, which may require remedial action on the RealPresence Resource Manager system.
Alert 2002
The cluster responsible for RealPresence Resource Manager integration was unable to connect to the RealPresence Resource Manager system.

Resource management system <system-name> unreachable. Last contact on: YYYY-MM-DD HH:MM GMT+/-H[;MM].
This may indicate a network problem or a problem with the RealPresence Resource Manager system.
Try logging in to the RealPresence Resource Manager system. If you can do so, make sure the login credentials that the RealPresence DMA system uses to connect to it are still valid.

Alert 2004
The system is integrated with a RealPresence Resource Manager system, and there is a problem with the territory definitions or responsibility assignments in the site topology data imported from that system.

Resource management server <system-name> has inconsistent territory definitions in its site topology.
On the RealPresence Resource Manager system, configure territories properly (for instance, no duplicate names) and in a way that meets the needs of the RealPresence DMA system. Assign responsibilities (primary and backup) for the territories to the appropriate RealPresence DMA clusters. A territory can only host conference rooms if it's assigned to a RealPresence DMA cluster.

Active Directory Integration
The following alerts provide information on changes in Active Directory integration status.

Alert 2101
The cluster responsible for Active Directory integration was unable to update the cache of user and group data.

Active Directory user and group cache update was not successful on cluster <cluster>.
This may indicate a network problem or a problem with the AD.
If the cluster was unable to log in to the AD server, alert 2107 is also generated.
Click the link to go to the Microsoft Active Directory page and check the Active Directory Connection section.

Alert 2102
The cluster responsible for Active Directory integration successfully retrieved user and group data, but no conference rooms were generated.

Zero enterprise conference rooms exist on cluster <cluster>.
This may indicate that no directory attribute was specified from which to generate conference room IDs, or that the chosen attribute resulted in empty (null) conference room IDs after the system removed the characters to remove.
Click the link to go to the Microsoft Active Directory page and check the Enterprise Conference Room ID Generation section. If necessary, check the Active Directory and determine an appropriate directory attribute to use.

**Alert 2104**

The primary and backup cluster for the territory responsible for Active Directory integration are both unreachable.

**Active Directory service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.**

This may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).

Click the link to go to the DMAs page to begin troubleshooting. Determine whether the clusters were deliberately shut down. If not, try pinging the clusters’ IP addresses.

Other clusters can continue using the shared data store from the last cache update, so there is no immediate AD-related problem. But the unavailable clusters probably have other territory-related responsibilities (conference manager and/or call server), so you may need to assign the affected territory to some other cluster(s).

**Alert 2105**

The primary cluster for the territory responsible for Active Directory integration is unreachable, and it has no backup cluster.

**Active Directory service is not available. Cluster <p-cluster> is not operational.**

This may indicate a network problem. It is also possible that someone shut the cluster down or that it failed.

Click the link to go to the DMAs page to begin troubleshooting. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster’s IP addresses.

Other clusters can continue using the shared data store from the last cache update, so there is no immediate AD-related problem. But the unavailable cluster probably has other territory-related responsibilities (conference manager and/or call server), so you may need to assign the affected territory to some other cluster.

Polycom recommends assigning a backup cluster for each territory.

**Alert 2106**

The specified server tried to connect to the Active Directory in order to authenticate a user's credentials and was unable to do so.

**Cluster <cluster>: Failed connection from <server> to Active Directory for user authentications at YYYY-MM-DD HH:MM GMT+/H[:MM].**

This may indicate a network problem or a problem with the AD itself.

If the network and the AD itself both appear to be OK, the connection attempt may have failed because the cluster was unable to log in to the AD server.

Click the link to go to the Microsoft Active Directory page. Make sure the login credentials that the RealPresence DMA system uses to connect to Active Directory are still valid and update them if necessary.
Alert 2107
The cluster responsible for Active Directory integration was unable to log into the AD server.

Failed connection from <cluster> to Active Directory for user caching at YYYY-MM-DD HH:MM GMT+/-H[:MM].
Click the link to go to the Microsoft Active Directory page.

Alert 2108
The territory's primary cluster assigned to do Active Directory integration is not reachable.

<alerting-cluster>: Active Directory primary cluster <p-cluster> associated with territory <territory> is not reachable. But backup cluster <c-cluster> is reachable.
The territory's backup cluster assigned to do Active Directory integration is reachable.
This may indicate a network problem. It's also possible that someone shut the primary cluster down or that it failed.
Click the link to go to the Integrations > DMA page. Log in to the affected cluster, if possible, and check the health of the cluster. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster's IP addresses.

Exchange Server Integration
The following alerts provide information on changes in Exchange server integration status.

Alert 2201
The primary cluster for the territory responsible for Exchange server integration is unreachable, and its backup cluster has taken over responsibility for monitoring the Polycom Conferencing user mailbox and accepting or declining the meeting invitations received.

Exchange server integration primary cluster <p-cluster> is not operational. Integration by backup cluster <b-cluster>.
This may indicate a network problem. It's also possible that someone shut the cluster down or that it failed.
Click the link to go to the DMAs page to begin troubleshooting.

Alert 2202
The primary and backup clusters for the territory responsible for Exchange server integration are both unreachable.

Exchange server integration is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.
This may indicate serious network problems. It is also possible that someone shut both clusters down, or shut down one and the other then failed, or both failed (unlikely).
Click the link to go to the DMAs page to begin troubleshooting. Determine whether the clusters were deliberately shut down. If not, try pinging the clusters' IP addresses.

**Alert 2203**

The primary cluster for the territory responsible for Exchange server integration is unreachable, and it has no backup cluster.

*Exchange server integration is not available. Cluster <p-cluster> is not operational.*

This may indicate a network problem. It's also possible that someone shut the cluster down or that it failed.

Click the link to go to the DMAs page to begin troubleshooting.

**Database Status**

The following alerts provide information on database events and changes in database status.

**Alert 2401**

The specified cluster is unable to communicate with its shared call history database.

*Connection to the history/audit database for cluster <cluster> has failed.*

This may indicate a network problem, or a software failure within the cluster. The server(s) may need to be rebooted.

Go to the DMAs page to begin troubleshooting.

**Alert 2402**

The specified cluster is unable to communicate with its shared configuration database.

*Connection to the configuration database for cluster <cluster> has failed.*

This may indicate a network problem, or a software failure within the cluster. The server(s) may need to be rebooted.

Go to the DMAs page to begin troubleshooting.

**Skype for Business Integration**

The following alerts provide information on changes in Microsoft Skype for Business integration.
Alert 2601
The cluster cannot communicate with the specified Skype for Business server at the currently configured Next hop address.

Cluster <cluster>: Cannot reach Lync server <lyncserver> for presence publishing.
This could indicate a network problem, or a problem with the Skype for Business server.
Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try to ping the Skype for Business server's Next hop address to verify basic connectivity.

Alert 2602
The cluster cannot authenticate with the specified Skype for Business server; presence will not be published for Polycom conference contacts.

Cluster <cluster>: Cannot authenticate with <lyncserver> for presence publishing.
This could indicate incorrect RealPresence DMA system or Skype for Business server configuration. Begin troubleshooting by verifying that the Presence Publishing settings on the Service Config > Conference Manager Settings > Conference Settings page are correct.
Click the link to go to the Integrations > External SIP Peers page.

Alert 2603
The system is unable to authenticate with the Skype for Business server using the currently configured Skype for Business account URI.

Cluster <cluster>: Invalid Lync account URI configured for Lync server <lyncserver>.
Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try reentering the Skype account URI for the Skype for Business server on the Skype Integration tab.

Alert 2604
The system is unable to connect to the specified Skype for Business server at the currently configured Next hop address.

Cluster <cluster>: Cannot reach Lync server <lyncserver> to resolve conference IDs for RealConnect conferences.
Attempts to connect to a Skype for Business conference through the RealPresence DMA system will fail.
This could indicate a network problem, or that someone has shut down the Skype for Business server.
Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Try pinging the specified Skype for Business server's IP address. If it is reachable, verify that the Next hop address, Port, and Transport type settings on this page are correct.
Alert 2605
The system cannot authenticate with the specified Skype for Business server, preventing RealConnect conference ID resolution.

Cluster <cluster>: Cannot authenticate with <lyncserver> to resolve conference IDs for RealConnect conferences.
Attempts to connect to RealConnect conferences through the RealPresence DMA system will fail.
Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. Verify that the Transport Type is set to TLS, and that the Skype account URI on the Skype Integration tab is correct. If the RealPresence DMA system configuration is correct, investigate the Skype for Business server's configuration.

Signaling
The following alerts provide information on signaling events and changes in signaling status.

Alert 3001
The specified cluster does not have signaling enabled and is unable to accept calls.

No signaling interface enabled for cluster <cluster>. SIP, H.323, or WebRTC must be configured to allow calls.
To use the cluster for anything other than logging into the management interface, you must enable signaling.
If you are logged in to that cluster, click the link to go to the Signaling Settings page. If not, log into that cluster and go to Admin > Server > Signaling Settings.

Certificate
The following alerts provide information on changes in certificate status such as certificate expirations and incompatibilities.

Alert 3101
The specified cluster's server certificate has expired.

Cluster <cluster>: The server certificate has expired.
This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. The cluster can no longer communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.
If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster (your browser will warn you not to do this, and you will have to override its advice) and go to Admin > Server > Certificates.
Alert 3102
The specified cluster's server certificate is about to expire.

Cluster <cluster>: The server certificate will expire within 1 day. All system access may be lost.
This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. If you allow it to expire, the cluster will no longer be able to communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.
If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.

Alert 3103
The specified cluster's server certificate will soon expire.

Cluster <cluster>: The server certificate will expire within <count> days. All system access may be lost.
This is the public certificate that the cluster uses to identify itself to devices configured for secure communication. If you allow it to expire, the cluster will no longer be able to communicate with any such devices, including MCUs, endpoints, the AD server, and the Exchange server.
If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.

Alert 3104
The specified cluster has an expired CA certificate or certificates.

Cluster <cluster>: One or more CA certificates have expired.
When a CA certificate expires, the certificates signed by that certificate authority are no longer accepted. Depending on its security settings, the cluster may refuse connections from devices presenting a certificate signed by a CA whose certificate has expired, including MCUs, endpoints, the AD server, and the Exchange server.
If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.
If that cluster has Skip validation of certificates for inbound connections turned off, you will not be able to log into it. Contact Polycom Global Services.

Alert 3105
The specified cluster has a CA certificate or certificates that will expire soon.

Cluster <cluster>: One or more CA certificates will expire within 30 days.
When a CA certificate expires, the certificates signed by that certificate authority are no longer accepted. If you allow the CA certificate(s) to expire, depending on its security settings, the cluster may refuse connections from any devices presenting a certificate signed by a CA whose certificate has expired, including MCUs, endpoints, the AD server, and the Exchange server.
If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates.
Alert 3108
The specified server's SSL certificate does not match the cluster's domain information or other network configuration.

Cluster <cluster>: The server SSL certificate is incompatible with the cluster's network settings. Perhaps the network configuration was changed, and the SSL certificate is now out of date.

If you are logged in to that cluster, click the link to go to the Certificates page. If not, log in to that cluster and go to Admin > Server > Certificates. Try regenerating the SSL certificate in question.

Licenses
The following alerts provide information on changes in licensing status.

Alert 3201
You have not entered the license key(s) for the specified cluster.

Cluster <DMA URL> has no license. Depending on the configuration, this DMA may borrow licenses from another DMA or you may install licenses from the Licenses page.

If you are logged in to the cluster, click the link to go to the Licenses page. If not, log in to the cluster and go to Admin > Server > Licenses.

Without a valid license, the cluster is limited to 10 simultaneous calls.

Alert 3202
The specified cluster has an invalid license key or keys.

Invalid license key(s) applied to cluster <cluster>. System will allow up to 10 concurrent calls.

If you are logged in to that cluster, click the link to go to the Licenses page. If not, log in to that cluster and go to Admin > Server > Licenses.

Without a valid license, the cluster is limited to 10 simultaneous calls.

Alert 3203
The system version has changed, and the End User License Agreement has not yet been accepted.

The EULA for cluster <cluster> has not been accepted. All calls are blocked on this cluster.

The specified cluster will not accept any inbound calls or place outbound calls, until a user with Administrator privileges accepts the agreement upon login.

Click the link to go to the Licenses page, where you can view the EULA acceptance status and details.
Alert 3204

The specified cluster cannot connect to the licensing server, or there is no licensing server configured for this cluster.

Cluster <cluster>: Cannot connect to licensing server <lserver>.

If you are logged in to that cluster, click the link to go to the Licenses page to view licensing details. Check the status of licensing by logging in to the RealPresence Platform Director system.

Alert 3205

The specified cluster's version of software is not compatible with the installed license.

Cluster <cluster>: DMA VE Soft RPP version is incompatible with license. No calls are permitted. Depending on the configuration, this DMA may borrow licenses from another DMA or you may install licenses from the Licenses page.

The system won't allow calls until you install a license that has been activated for this version of software. Click the link to go to the Licenses page to install the proper license activation key.

Alert 3206

The current license for the specified cluster doesn't support calls.

Cluster <cluster>: DMA is not licensed for any calls. Depending on the configuration, this DMA may borrow licenses from another DMA or you may install licenses from the Licenses page.

Click the link to go to the Licenses page to view licensing details or install a different license activation key.

Alert 3209

The current license for the specified cluster doesn't support concurrent VMRs.

Cluster <cluster>: DMA is not licensed for any VMRs. Depending on the configuration, this DMA may borrow licenses from another DMA or you may install licenses from the Licenses page.

Click the link to go to the Licenses page to view licensing details or install a different license activation key.

Networks

The following alerts provide information on network errors and connectivity.
Alert 3301

One of the servers in the specified cluster is not responding to the other server over the private network that connects them.

Cluster <cluster> is configured for 2 servers, but only a single server is detected.

This could be a hardware problem, or the server in question may just need to be rebooted. It is also possible that the private network connection between the two servers has failed. Check the Ethernet cable connecting the GB 2 ports (Polycom Rack Server 630 or 620-based systems) or the Port 1 ports (Polycom Rack Server 220-based systems) and replace it if necessary.

Alert 3302

Either the cluster contains two servers but was incorrectly configured as a single-server cluster, or there is only one server in the cluster but something is connected its GB 2 port (Polycom Rack Server 630 or 620-based systems) or Port 1 port (Polycom Rack Server 220-based systems).

Cluster <cluster> is configured for 1 server, but the private network interface is enabled and active.

On a single-server cluster, do not use the server's GB 2 port (Polycom Rack Server 630 or 620-based systems) or Port 1 port (Polycom Rack Server 220-based systems) for anything.

Alert 3303

The specified server has detected a problem with the private network that connects the two servers in the cluster.

Cluster <cluster>: A private network error exists on <server>.

For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 2 Ethernet port (eth1 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the Port 1 Ethernet port (eth1 interface).

This could also be a problem with the Ethernet cable connecting the eth1 interfaces of the two systems. Or, the server in question may just need to be rebooted.

Alert 3304

The specified server has detected a problem with the management (or combined management and signaling) network connection.

Cluster <cluster>: A public network error exists on <server>.

For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 1 Ethernet port (eth0 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the Port 0 Ethernet port (eth0 interface).

This could also be a problem with the Ethernet cable connecting the server to the enterprise network switch, or that switch.

Or, the server in question may just need to be rebooted.
Alert 3305
The specified server has detected a problem with the signaling network connection.

Cluster <cluster>: A signaling network error exists on <server>.
For systems installed on a Polycom Rack Server 630 (R630) or 620 (R620), this could be a problem with the GB 3 port (eth2 interface). For systems installed on a Polycom Rack Server 220 (R220), this could be a problem with the GB 1 port (eth2 interface).
This could also be a problem with the Ethernet cable connecting the server to the enterprise network switch, or that switch. Or, the server in question may just need to be rebooted.

Alert 3306
The system has found issues with the DNS configuration on the Admin > Server > Network Settings page for the specified cluster.

DNS <address of DNS server> settings are inconsistent with network configuration on Cluster <cluster>: <issue-text>.
This could indicate one of the following possible problems:
- The virtual or management host name A or AAAA record configured in the specified DNS server is missing
- The virtual or management host name A or AAAA record configured in the specified DNS server references the incorrect address
The alert text describes the nature of the problem, which may require additional configuration of the DNS server(s) or network settings for the cluster.
Refer to the Polycom RealPresence DMA System Operations Guide for more information regarding DNS configuration.
Click the link to go to the Admin > Server > Network Settings page.

Alert 3309
One or more configured DNS servers are not responding to requests from the specified cluster.

Cluster <cluster>: DNS <address of DNS server> is unresponsive. <service> at <FQDN> <referenced by> {will use <IP address> | cannot be reached}.
The system will use the last cached IP address for the DNS server, but if no IP address is known, this DNS server is considered unreachable.
This could indicate a network problem, or that a DNS server is out of service.
Click the link to go to the Admin > Server > Network Settings page.

Alert 3310
The specified cluster cannot resolve the domain name of this Active Directory, MCU, ISDN gateway, or DMA cluster.

Cluster <cluster>: DNS <address of server> cannot resolve <FQDN>. <service> <referenced by> cannot be reached.
The specified service is currently unreachable.
This could indicate a network problem, or that the specified domain name entry is incorrect in the DMA cluster's configuration.

If the alert originated from a different cluster, log in to that cluster and go to the Admin > Server > Network Settings page to begin troubleshooting. If you are already logged in to the originating cluster, click the link to go to the Admin > Server > Network Settings page.

Server Resources

The following alerts provide information on changes in the resources of the server or cluster.

Alert 3401

The specified cluster is running out of disk space.

Cluster <cluster>: Available disk space is less than 15% on server <server>.

Suggestions for recovering and conserving disk space include:

- Delete backup files (after downloading them).
- Remove upgrade packages.
- History data is written to the backup file nightly. Reduce history retention settings so the same history data is not being repeatedly backed up.
- Roll logs more often (compressing the data) and make sure Logging level is set to Production.

Alert 3403

Log archives on the specified cluster exceed the capacity limit for logs.

Cluster <cluster>: Log files on server <server> exceed the capacity limit and will be purged within 24 hours.

After midnight, the system will delete sufficient log archives to get below the limit.

Click the link to go to the System Log Files page. We recommend routinely downloading archived logs and then deleting them from the system.

Alert 3404

Log archives on the specified cluster have reached the percentage of capacity that triggers an alert, set on the Alerting Settings page.

Cluster <cluster>: Log files on server <server> are close to capacity and may be purged within 24 hours.

Click the link to go to the System Log Files page. We recommend routinely downloading archived logs and then deleting them from the system.
Alert 3405
The specified server's CPU and/or I/O bandwidth usage is unusually high.

**Server <server> CPU utilization >50% and <75%.**
This can be caused by activities such as backup creation, CDR downloading, logging at too high a level, or refreshing an extremely large Active Directory cache.

The cause may also be a system health problem or a runaway process. Go to Admin > Troubleshooting Utilities > Top to see if a process is monopolizing CPU resources.

Create a new backup and download it, and then contact Polycom Global Services.

Alert 3406
The specified server's CPU and/or I/O bandwidth usage is exceptionally high.

**Server <server> CPU utilization > 75%.**
This can be caused by activities such as backup creation, CDR downloading, logging at too high a level, or refreshing an extremely large Active Directory cache.

The cause may also be a system health problem or a runaway process. Go to Admin > Troubleshooting Utilities > Top to see if a process is monopolizing CPU resources.

Create a new backup and download it, and then contact Polycom Global Services.

Data Synchronization
The following alerts provide information on changes in data synchronization between servers in the cluster.

Alert 3601
The specified cluster is supposed to have two servers, but a software version mismatch makes it impossible for them to form a redundant two-server cluster.

**Cluster <cluster>: System version differs between servers.**
Possible explanations:

- Someone upgraded one server of the cluster while the other was turned off or otherwise unavailable.
- An expansion server was added to a single-server cluster, but the new server was not patched to the same software level as the existing server.
- An RMA replacement server was not patched to the same software level as the existing server.

If you are logged in to that cluster, click the link to go to the Software Upgrade page. If not, log in to that cluster and go to Admin > Software Upgrade. Check Operation History.

Log into the physical address of the server that was unable to join the cluster and upgrade it to match the other server. After it restarts, it will join the cluster.
Alert 3602
The time on the two servers in the specified cluster has drifted apart by an unusually large amount.

Cluster <cluster>: Local time differs by more than ten seconds between servers.
This may indicate a configuration issue or a problem with one of the servers. Contact Polycom Global Services.

Alert 3603
In the specified cluster, the Active Directory integration status information is different on the two servers, indicating that their internal databases are not consistent.

Cluster <cluster>: Active Directory integration is not consistent between servers.
Try to determine which server's data is incorrect and reboot it.

Alert 3604
In the specified cluster, the enterprise conference room counts are different on the two servers, indicating that their internal databases are not consistent.

Cluster <cluster>: Enterprise conference rooms differ between servers.
Try to determine which server's data is incorrect and reboot it.

Alert 3605
In the specified cluster, the custom conference room counts are different on the two servers, indicating that their internal databases are not consistent.

Cluster <cluster>: Custom conference rooms differ between servers.
Try to determine which server's data is incorrect and reboot it.

Alert 3606
In the specified cluster, the local users are different on the two servers, indicating that their internal databases are not consistent.

Cluster <cluster>: Local users differ between servers.
Try to determine which server's data is incorrect and reboot it.

System Health and Availability
The following alerts provide information on changes in the health and availability of the system.
Alert 3801
The cluster from which the alert originated is reporting that a server in a different cluster has failed over to an alternate server because of an internal software component failure.

<d-cluster>: Cluster <f-cluster>/server <f-server> failover to <b-server> due to <component> failure: <details of failure>
The alert includes details on what component experienced the failure.
This alert is cleared when the condition that caused the alert is resolved.
Use the failure details as a starting point for troubleshooting. If the failure is not hardware or network related, and you are unable to access the server, it may need to be rebooted.
Click the link to go to the Integrations > DMA page.

Alert 3802
The cluster from which the alert originated is reporting that a server in a different cluster has restarted because of an internal component failure.

<d-cluster>: Cluster <f-cluster>/server <f-server> restarted due to <component> failure: <details of failure>
The alert includes details on what component experienced the failure.
Use the failure details as a starting point for troubleshooting. If the failure is not hardware or network related, and you are unable to access the server, it may need to be physically powered off and powered back on.
Click the link to go to the Integrations > DMA page.

Alert 3803
The cluster from which the alert originated is reporting that a server in a different cluster has experienced one or more software component issues, and is running in an unhealthy state.

<d-cluster>: Cluster <f-cluster>/server <f-server> is operating in an impaired state due to <component> issue: <details of impairment>
The alert includes further details of the impairment of the system.
Use the impairment details as a starting point for troubleshooting. If the impairment is not hardware or network related, and you are unable to access the server, it may need to be rebooted.
Click the link to go to the Integrations > DMA page.

Cluster Features
The following alerts provide information on the status of certain cluster operations.
Alert 3901
The specified cluster could not resolve the hostname or IP address of the remote backup server, causing the backup scheduled at <date-time> to fail.

<cluster>: Scheduled backup at <date-time> failed because the remote server address could not be resolved.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.
Click the link to go to the Admin > Server > Backup Settings page. Ensure the hostname or IP address for the remote backup server is correct, and that the server is reachable from the RealPresence DMA system.

Alert 3902
The specified cluster did not receive a response from the configured remote backup server, causing the backup scheduled at <date-time> to fail.

<cluster>: Scheduled backup at <date-time> failed because there was no response from the remote server.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.
Click the link to go to the Admin > Server > Backup Settings page.

Alert 3903
The specified cluster was unable to authenticate with the configured remote backup server using the configured login and password, causing the backup scheduled at <date-time> to fail.

<cluster>: Scheduled backup at <date-time> failed because the configured login/password for the remote server are invalid.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.
Click the link to go to the Admin > Server > Backup Settings page. Ensure the credentials for the remote backup server are correct.

Alert 3904
A communications error with the backup server caused the backup scheduled at <date-time> to fail.

<cluster>: Scheduled backup at <date-time> failed because there was a data transfer error with the remote server.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.
Click the link to go to the Admin > Server > Backup Settings page. Ensure the network link between the RealPresence DMA system and the remote backup server is reliable.
Alert 3905
The RealPresence DMA system was unable to create the backup file on the remote backup server, causing the backup scheduled at <date-time> to fail.

<cluster>: Scheduled backup at <date-time> failed because the backup file could not be created.
This alert is cleared the next time a scheduled backup is successful, regardless of any configuration changes.
Click the link to go to the Admin > Server > Backup Settings page. Check the remote backup server's file system permissions to ensure the RealPresence DMA system can create and write to files there.

MCUs
The following alerts provide information on changes in the status of connected MCUs.

Alert 4001
Someone busied out the specified MCU.

MCU <MCUname> is currently busied out.
Click the link to go to the Integrations > MCU page.

Alert 4002
Someone took the specified MCU out of service.

MCU <MCUname> is currently out of service.
Click the link to go to the Integrations > MCU page.

Alert 4003
The MCUs page is displaying warnings related to the specified MCU.

MCU <MCUname> has <count> warning(s).
Click the link to go to the Integrations > MCU page for more information.

Alert 4004
The system was unable to establish an additional management session connection to the specified MCU.

MCU <MCUname> is configured with insufficient user connections.
Possible explanations:
- IP connectivity between the system and the MCU has been lost.
- This MCU does not allow sufficient connections per user.

Polycom MCUs use synchronous communications. In order to efficiently manage multiple calls as quickly as possible, the RealPresence DMA system uses multiple connections per MCU. By default, a
RealPresence Collaboration Server or RMX MCU allows up to 20 connections per user (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). We recommend not reducing this setting. If you have a RealPresence DMA supercluster with three conference manager clusters and a busy conferencing environment, we recommend increasing this value to 30.

After a connection attempt fails and this alert is triggered, the system tries every 60 seconds to establish five connections to this MCU. If it succeeds, this alert is automatically cleared.

Click the link to go to the Integrations > MCU page.

Alert 4005
The reporting cluster is unable to connect to the specified MCU.

MCU <MCUname> is disconnected.
This may indicate a network problem. It is also possible that someone shut the MCU down or that it failed.
Click the link to go to the Integrations > MCU page for more information.

Alert 4009
The RealPresence DMA cluster has lost connection with the specified MCU between one and four times in the past 24 hours.

MCU <mcu> disconnect rate is > 1 and < 4.
This most likely indicates a network problem, but it could also indicate that the MCU or RealPresence DMA system is under very heavy load. If the MCU stays connected for more than 24 hours, this alert is cleared, but if the RealPresence DMA system loses connection with this MCU more than four times in 24 hours, this alert is replaced with Alert 4010.

Click the link to go to the Integrations > MCU page to begin troubleshooting. Check the network connection between this MCU and the RealPresence DMA cluster.

Alert 4010
The DMA cluster has lost connection with the specified MCU more than four times in the past 24 hours.

MCU <mcu> disconnect rate is > 4.
This most likely indicates a network problem, but it could also indicate that the MCU or RealPresence DMA system is under very heavy load.

Click the link to go to the Integrations > MCU page to begin troubleshooting. Check the network connection between this MCU and the RealPresence DMA cluster.

Alert 4011
The specified MCU's number of consecutive failed calls has changed, and the calculated failure penalty metric is now between 0.4 (some calls are failing) and 0.8 (most calls are failing).

MCU <mcu> call failure penalty is > 0.4 and < 0.8.
The RealPresence DMA system keeps track of per-MCU call failure penalties not only to alert administrators to call failures, but also to ensure that calls will be routed less often to MCUs with high call failure penalties.
Alerts

Click the link to go to the **Integrations** > **MCU** page to begin troubleshooting.

**Related Links**

[MCU Availability and Reliability Tracking](#) on page 192

**Alert 4012**

The specified MCU's number of consecutive failed calls has changed, and the calculated failure penalty metric is now above 0.8.

**MCU <mcu> call failure penalty is > 0.8.**

This indicates that most of the specified MCU's calls are failing. The RealPresence DMA system keeps track of per-MCU call failure penalties not only to alert administrators to call failures, but also to ensure that calls will be routed less often to MCUs with high call failure penalties.

Click the link to go to the **Integrations** > **MCU** page to begin troubleshooting.

**Related Links**

[MCU Availability and Reliability Tracking](#) on page 192

**Alert 4013**

The specified MCU has no ports available for call traffic.

**MCU <mcu> is connected with no port capacity.**

This could indicate that the specified MCU is at capacity, or possibly a network problem. This alert appears as soon as the port capacity of this MCU becomes 0, and is automatically cleared after 2 minutes.

Click the link to go to the **Integrations** > **MCU** page to begin troubleshooting.

**Alert 4014**

The video port capacity of the specified MCU has changed.

**MCU <mcu> video port capacity changed from <oldcapacity> to <newcapacity>.**

This could indicate a license change, video/voice port configuration change, or hardware change for the MCU (perhaps a media card has been removed or added). This alert appears as soon as the video port capacity of this MCU becomes 0, and is automatically cleared after 2 minutes.

Click the link to go to the **Integrations** > **MCU** page.

**Alert 4015**

The voice port capacity of the specified MCU has changed.

**MCU <mcu> voice port capacity changed from <oldcapacity> to <newcapacity>.**

This could indicate a license change, video/voice port configuration change, or hardware change for the MCU (perhaps a media card has been added or removed). This alert appears as soon as the voice port capacity of this MCU becomes 0, and is automatically cleared after 2 minutes.

Click the link to go to the **Integrations** > **MCU** page.
Alert 4016
The specified MCU has been automatically busied out because it failed to start <N> number of conferences in a row.

MCU <mcu> has been automatically busied out due to <N> consecutive failures to start conferences. Investigate the MCU state and logs.
This condition is likely caused by an MCU software issue. Non-consecutive failures to start calls do not trigger this condition.
Once the MCU is busied out, when the last conference ends on the MCU, the MCU automatically changes to the Out of Service state. Once that happens, this alert is replaced with alert 4017.
Click the link to go to the Integrations > MCU page.

Alert 4017
The specified MCU has been placed in the Out of Service state after it was automatically busied out because it failed to start <N> number of conferences in a row.

MCU <mcu> has been automatically placed out of service due to <N> consecutive failures to start conferences. Investigate the MCU state and logs.
This condition is likely caused by an MCU software issue.
This alert replaces alert 4016.
Click the link to go to the Integrations > MCU page.

Alert 4018
The Media Control Channel Framework (MCCF) connection limit for the specified MCU has been exceeded, because there are too many RealPresence DMA systems connecting to this MCU.

MCU <mcu> MCCF connection limit exceeded. Some conference features will not work.
Additional RealPresence DMA systems will connect to this MCU without MCCF, but some IVR, VEQ, passcode, and CDR features will not work correctly.
To correct this problem, reduce the number of RealPresence DMA systems simultaneously connecting to this MCU.
Click the link to go to the Network > MCU > MCUs page.

Endpoints
The following alerts provide information on communication issues with endpoints.
Alert 5001
A device that identifies itself as an Immersive Telepresence (ITP) system has registered with the call server, but the H.323 ID or SIP URI of the device doesn't specify its endpoint number or the number of endpoints in the ITP system, as it should.

<Model> ITP system attempting to register with ID <H.323 ID or SIP URI> is improperly configured.
The H.323 ID or SIP URI must be updated on the endpoints of the ITP system.

Related Links
Naming ITP Systems for Recognition by the RealPresence DMA System on page 531

Alert 5002
At least one device, in violation of protocol standards, is sending too much of the specified type of signaling traffic (H.323 or SIP) to the RealPresence DMA system.

One or more endpoints are sending too much <signaling_type> signaling traffic. They have been temporarily blacklisted and may have been quarantined.
If there are many such ill-behaved devices, it could affect the RealPresence DMA system's ability to provide service, so the system temporarily blacklists any such device (ignoring all signaling from it until it stops sending messages more frequently than the specification permits). Depending on the registration policy, it could also be quarantined, and it remains so until manually removed from quarantine.

Click the link to go to the Network > Endpoints page, where you can search for endpoints with Registration status of Quarantined or Quarantined (Inactive).

Alert 5003
The specified device has unregistered or its registration has expired.

The <device model> device identified by [device identifier] is no longer registered to the call server.
This alert appears only if it has been enabled for this endpoint or MCU. This alert is automatically cleared after 2 minutes.
Click the link to go to the Endpoints page.

Alert 5004
As the system tried to route the H.323 or SIP call from its source to the destination, a dialing loop in the site topology was detected, and the call was dropped.

<sigtype> call from <originator> to <dial string> was dropped due to routing loop.
Click the link to go to the Reports > Call History page and view more information about the call.

Related Links
Suggestions for Modifying the Default Dial Plan on page 307
Conference Manager

The following alerts provide information on possible problems with conference manager functionality.

Alert 6001

You must enable a territory to host conference rooms in order to use the cluster responsible for the territory as a conference manager.

No territories configured to host conference rooms.
You can enable up to three territories to host conference rooms.
Click the link to go to the Service Config > Site Topology > Territories page.

Alert 6002

The specified entry queue used by the VEQ <VEQnum> is not configured on an MCU.

Shared number dialing VEQ <VEQnum> references entry queue <EQname> which is not configured on any MCUs.
If the VEQ is a Direct Dial VEQ, <VEQnum> is Direct Dial.
Click the link to go to Service Config > Conference Manager Settings > Shared Number Dialing to begin troubleshooting. Ensure that at least one MCU configured in Integrations > MCU has the specified entry queue configured.

Related Links
Shared Number Dialing on page 278

Conference Status

The following alerts provide information on some types of call failures.

Alert 6101

A preset dialout from the conference using the conference room identifier <VMR> has failed for the specified reason.

Call failed: Preset dialout from conference VMR <VMR> to <destination> failed. Cause: <cause>
This alert automatically clears after 2 minutes.
Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.
Alert 6102
A conference using the conference room identifier <VMR> has failed to start for the specified reason.

Conference <VMR> on MCU <MCU> failed to start: <reason>.
If no MCU was selected, <MCU> is unresolved. This alert automatically clears after 2 minutes.
Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6103
A conference using the conference room identifier <VMR> has been aborted for the specified reason.

Ongoing conference <VMR> on MCU <MCU> failed: <reason>.
This alert automatically clears after 2 minutes.
Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6104
A conference using the conference room identifier <VMR> has been moved from <MCU1> to <MCU2> for the specified reason.

Ongoing conference <VMR> on MCU <MCU1> failed over to MCU <MCU2>: <reason>.
This alert automatically clears after 2 minutes.
Click the link to go to the Network > Users page to find the specified VMR number and begin troubleshooting.

Alert 6105
The system is unable to find the specified OU in Active Directory, and will be unable to start RealConnect conferences using external Lync systems.

Integrations > Microsoft Active Directory > Lync RealConnect Callback contacts OU value, '<OU>', does not exist in Active Directory.
When you integrate with an external Lync system, the RealPresence DMA system uses an Active Directory contact from the OU specified in this field to receive calls forwarded from the external Lync system.
Click the link to go to the Integrations > Microsoft Active Directory page. Verify that the value for the Callback contacts OU field is correct and contains valid contacts that the system can use for this purpose.
Alert 6106
The system is unable to find any callback contacts to use in the OU specified on the Integrations > Microsoft Active Directory page.

RealConnect conference with external Lync system cannot start. There are no available callback contacts.
RealConnect conferences with external Skype for Business systems will not start.
When you integrate with an external Skype for Business system, the RealPresence DMA system uses an Active Directory contact from the OU specified on this page to receive calls forwarded from the external Skype for Business system.
Click the link to go to the Integrations > Microsoft Active Directory page. Verify that the value for the Callback contacts OU field is correct and contains valid contacts that the system can use for this purpose.

Alert 6107
The system is unable to create a conference because the maximum number of dynamic conference IDs have been generated.

Conference factory - all generated dynamic conference IDs are in use.

Alert 6108
The system is unable to create a conference because protection against Denial of Service (DOS) attacks has been activated.

Conference factory - too many conference factory requests received.

Skype for Business Presence Publishing
The following alerts provide information on problems the system may encounter when publishing presence for Polycom conference contacts.

Alert 6201
The system was unable to publish presence status for the specified number of Polycom conference contacts because the Skype for Business server has been configured with a maximum endpoint logon period of <expire> seconds.

Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>. Presence for <NN> of <MM> Polycom conference contacts will not be published due to Lync server configuration 'MaxEndpointExpiration' value <expire>.

To publish presence status for Polycom conference contacts, the system registers each contact with the Skype for Business server every 'MaxEndpointExpiration' seconds. Depending on how many conference contacts are configured for presence publishing, the RealPresence DMA system may be unable to publish presence for all contacts during this interval, as the system registers one conference contact per second.
If suitable for your environment, either increase the 'MaxEndpointExpiration' value on the Skype for Business server, or decrease the number of Polycom conference contacts configured for publishing.

Click the link to go to the Integrations > External SIP Peers page.

**Alert 6202**

The system was unable to publish presence status for the specified number of Polycom conference contacts because the **Maximum Polycom conference contacts to publish** value configured in the Skype for Business server's External SIP Peer properties has been reached.

Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>. Presence for <NN> of <MM> Polycom conference contacts will not be published because the number of Polycom conference contacts configured for publishing exceeds 'Maximum Polycom conference contacts to publish' configured on the system.

Click the link to go to the Integrations > External SIP Peers page to begin troubleshooting. If suitable for your environment, increase the **Maximum Polycom conference contacts to publish** value.

**Alert 6203**

The system was unable to publish presence status for the specified number of Polycom conference contacts within the number of seconds specified by the **MaxEndpointExpiration** setting on the Skype for Business server.

Cluster <cluster>: Errors in presence publication for Lync server <lyncserver>. Presence for <NN> of <MM> Polycom conference contacts will not be published: the system is unable to complete publication within the expiration interval.

To publish presence status for Polycom conference contacts, the RealPresence DMA system registers each contact with the Skype for Business server every **MaxEndpointExpiration** seconds. This alert could indicate heavy RealPresence DMA system load or other performance-related factors during presence publishing.

If suitable for your environment, either increase the **MaxEndpointExpiration** value on the Skype for Business server, or decrease the number of Polycom conference contacts configured for publishing.

Click the link to go to the Integrations > External SIP Peers page.

**Alert 6205**

The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the system time differs between the RealPresence DMA system and the Active Directory system.

Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; DMA time is skewed from Active Directory's time.

If possible, ensure that the RealPresence DMA system and your Active Directory system both use the same NTP server.

Click the link to go to the Integrations > Microsoft Active Directory page.
Alert 6206
The specified cluster has attempted to create or manage Active Directory conference contacts, and failed.

Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; DNS cannot resolve the "<setting>", <FQDN>, configured at <page>.

The cluster either cannot resolve the IP address or host name configured on the Integrations > Microsoft Active Directory page, or the Next hop address configured for the specified SIP peer on the Integrations > External SIP Peers page.

Go to the page specified in the alert, and verify that the configuration is correct. If so, verify your network's DNS configuration.

Click the link to go to the page specified in the alert.

Alert 6207
The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the domain, user name, or password is incorrect on the Integrations > Microsoft Active Directory page.

Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; invalid domain, user name, or password.

Click the link to go to the Integrations > Microsoft Active Directory page, and verify that the Domain, Domain/user name, and Password fields are correct.

Alert 6208
The specified cluster has attempted to create or manage Active Directory conference contacts, and failed because the Active Directory system is not configured for Windows Remote Management.

Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; Active Directory is not configured for Windows Remote Management.

For details on enabling Windows Remote Management on your Active Directory system, refer to the Polycom Unified Communications for Microsoft Environments - Solution Deployment Guide.

Click the link to go to the Integrations > Microsoft Active Directory page.

Alert 6209
The specified cluster has attempted to create or manage Active Directory conference contacts, and failed.

Cluster <cluster>: Failed to create/manage conference contacts in Active Directory; Active Directory reports error: <text>.

The Active Directory system has reported <text> in response to the RealPresence DMA system's request. Use the error text to begin troubleshooting.

Click the link to go to the Integrations > Microsoft Active Directory page.
Call Server

The following alerts provide information on issues with call server functionality.

Alert 7001
Registration data retention settings are too low for the system to determine the number of failed registrations in the past 24 hours.

Failed registration data incomplete: cluster <cluster> history limited to <n.n> hours.
Click the link to go to the Admin > ServerHistory Retention Settings page and increase the number of registration records to retain on each cluster.

Alert 7005
The specified site is configured for automatic E.164 alias number assignment, but all of the aliases within the specified range are already assigned.

Site <sitename> has no available aliases for automatic ISDN assignment.
Click the link to go to the Service Config > Site Topology > Sites page to begin troubleshooting. Try expanding the ISDN number ranges specified in the site’s ISDN Range Assignment section.

Alert 7006
The specified cluster has detected that the external SIP peer named <sippeer> is not responding.

Cluster <cluster>: External SIP peer <sippeer> is unresponsive.
Click the link to go to the Integrations > External SIP Peers page to view the settings of the specified external SIP peer.

Call Bandwidth Management

The following alerts provide information on possible bandwidth management issues and other bandwidth management events.

Alert 7101
The DMA system has disallowed the specified number of calls <N> from starting, as there is not enough bandwidth to carry the calls on the site topology segment (subnet, site, or site link) with the name <throttlepoint>.

<N> Calls rejected starting at <time> due to lack of bandwidth on <throttlepoint-type> <throttlepoint>.
Click the link to go to the Reports > Call History page, where the first call to be rejected during this event is displayed. If possible in your environment, increase the bandwidth available to this subnet, site, or site link.
Troubleshooting Utilities

Topics:

- Run Network Packet Capture
- Run Ping
- Run Traceroute
- Run Top
- Run I/O Stats
- Run SAR
- Check NTP Status
- Manually Synchronize all Clusters
- Reset to Default Settings
- Diagnostics for your Polycom Server

The RealPresence DMA system includes various network and system troubleshooting utilities.

Run Network Packet Capture

Run Network Traffic Capture to capture data packets received or sent by the network interfaces on your RealPresence DMA system.

The traffic capture generates a packet capture (.pcap) file that contains the network traffic information.

If needed, you can apply a filter on the network interface for which you capture packets. Conditional statements determine which data is captured. For example, a filter might capture data coming from ABC route and having W.X.Y.Z IP address. Example filters include the following:

- host src, dst
- tcp, udp, icmp
- src port 1025 and tcp
- portrange 21-23
- src 10.0.1.1 and port 80
- src 10.0.2.1 and (dst port 3389 or 22)
- dst host 192.168.1.1 and (dst port 80 or dst port 443)

For a description of pcap filters see [http://www.tcpdump.org/manpages/pcap-filter.7.html](http://www.tcpdump.org/manpages/pcap-filter.7.html).

Procedure

1. Go to Admin > Troubleshooting Utilities > Network Packet Capture.
2. Enter a Pcap filter or accept the default to Capture all packets.
3. Select the Capture Interfaces for which to capture packets.
4. Click Capture to start the packet capture.
5. Click Stop to stop the capture.
The RealPresence DMA system generates a packet capture file with the .pcap extension and prompts you to download the file.

6. Go to Admin > System Log Files and select the .pcap file to download.
7. Click Download Individual Logs and select a location to save the file.

  The system notifies you when the download is complete.

Run Ping

Use the ping and arping commands to verify that a RealPresence DMA system can communicate with another device in the network.

You can run and see the results of the ping or arping command on each server in a cluster.

Ping and arping will verify communication with most devices in a network but are not foolproof commands. For example, if a device is offline but still active, or if it hasn't been used recently, it might not be found by using ping or arping.

Procedure

1. Go to Admin > Troubleshooting Utilities > Ping.
2. Enter an IP address or host name.
3. Select the Ping type the system will perform (ping or arping).
4. Optionally, select Use specified network interface and select a network interface from the drop-down list.
   The ping or arping request will originate from the IP address of the network interface you select.
5. Click Ping.

  The system displays the results of the command.

Run Traceroute

Use Traceroute to see the route that the system uses to reach the address you specify and the latency (round trip) for each hop.

Procedure

1. Go to Admin > Troubleshooting Utilities > Traceroute.
2. Enter an IP address or host name and click Trace.

  The system displays the results of the command.

Run Top

Use Top to see an overview of your RealPresence DMA system's current status, including CPU and memory usage, number of tasks, and list of running processes.

The results automatically update every few seconds and you can see the updated results of the top command for the system.

Procedure

  » Go to Admin > Troubleshooting Utilities > Top.
The system displays results of the command for each server.

Run I/O Stats

Run I/O Stats to see CPU resource allocation and read/write statistics for each RealPresence DMA system.

For detailed information about the output of this utility, refer to the utility documentation at http://sebastien.godard.pagesperso-orange.fr/man_iostat.html.

Procedure

» Go to Admin > Troubleshooting Utilities > I/O Stats.
   The system displays the results of the command.

Run SAR

Use SAR to see a complete system activity report (from the preceding midnight to the current time) for each RealPresence DMA system.

Procedure

» Go to Admin > Troubleshooting Utilities > SAR.
   The system displays the results of the command.

Check NTP Status

Use NTP Status to see a list of clock sources known to each server (including the local clock) and their status.

It runs the command ntpq -p on your RealPresence DMA system. For detailed information about the output of this utility, refer to the utility documentation at http://nlug.ml1.co.uk/2012/01/ntpq-p-output/831.

Procedure

» Go to Admin > Troubleshooting Utilities > NTP Status.
   The system displays the results of the command.

Manually Synchronize all Clusters

The Manually Synchronize all Clusters feature synchronizes system configuration data across all servers in the supercluster and automatically repairs synchronization issues.

When you change configuration settings on a RealPresence DMA system, the changes are first stored locally on one of the systems in the supercluster, and synchronized soon after with the other systems. At times (usually during severe network outages), a server can lose data and the configuration becomes inconsistent between systems in the supercluster. Nightly, each individual DMA system automatically performs a self-check on its data and will fix inconsistencies if found. Manually synchronizing initiates this process immediately and simultaneously on all DMA systems (standalone or HA nodes) in the supercluster.
Caution: This operation may take several minutes and may consume significant memory and CPU resources. Polycom does not recommend using this utility during peak traffic periods or while other resource-intensive tasks are underway (such as system backups, CDR downloads, or Microsoft Active Directory integration updates).

Procedure
1. Go to Admin > Troubleshooting Utilities > Manually Synchronize all Clusters.
2. Click OK to confirm the action.

Reset to Default Settings
A RealPresence DMA system can be reset back to its factory default configuration.

A reset will clear most settings you have configured on the User, Integrations, and Service Config menus, and some settings on the Admin menu in the management user interface. A reset will also change the management user interface administrator password back to the factory default, but will not reset the system root password.

You cannot reset a system to the default settings if it is enabled for High Availability or is part of a supercluster. You must first disable High Availability or remove the system from the supercluster.

If you reset the system to its default configuration, the following settings will not be reset and will remain the same after your system reboots:
- Network settings
- Time settings
- Licenses
- Logging settings
- Security settings
- Certificates
- SNMP settings
- Alert settings
- Backup settings
- EULA acceptance

Procedure
1. Go to Admin > Troubleshooting Utilities > Reset to Default Settings.
   The system displays a warning message.
2. Click OK to continue.
   The system displays a second warning message.
3. Click Yes to confirm.
   The system displays the login screen and then reboots with the default settings.
4. Log in with the factory-default credentials and reconfigure any changed settings as needed for your network environment.
Diagnostics for your Polycom Server

You should perform server diagnostics on your RealPresence DMA system hardware (Appliance Edition) only under the guidance of Polycom Global Services.

You need to have a monitor and USB keyboard to run the diagnostics.
RealPresence DMA System Network Configurations

Topics:

▪ Legend
▪ Core Configurations
▪ Edge Configurations
▪ Combination Configurations

When you install one or more RealPresence DMA systems, you need to configure each system with a core configuration, an edge configuration, or a combination configuration as follows:

▪ A core configuration is recommended if the system(s) is deployed inside your network environment.

▪ An edge configuration provides additional security features and is recommended if you deploy the system in the DMZ and it communicates with one or more core-configured systems inside your enterprise network.

▪ A combination system is one of the following:
  ◦ An edge-configured system that resides in the DMZ and doesn’t communicate with any core-configured system. The system can handle registrations, calls, firewall/NAT traversal, and conferences with virtual meeting rooms.
  ◦ An edge-configured system inside the enterprise that is part of a VPN tunnel and doesn’t communicate with any core-configured system. The system can handle registrations, calls, and conferences with virtual meeting rooms.

The following diagrams show potential network configurations.

Legend

-------- Communication between DMA and other non-DMA components

----------- Communication between DMAs

----------- HA/Supercluster Communication between DMAs
Core Configurations

Single Core System to Edge System

Active-Passive HA Core Systems to Edge System
Active-Active HA Core Systems to Edge System

Supercluster with Single Core System to Edge System
Supercluster with Active-Passive HA Core Systems to Edge System

Edge Configurations

Single Edge System to Core System
Active-Passive HA Edge Pair to Core System

Active-Active HA Edge Pair to Core System
VPN Tunnel Between Edge System and Combination System

VPN Tunnel Between Two Edge Systems Communicating with Core System
Combination Configurations

Edge System, No Core System

Diagram: Network configuration with DMZ and firewall.
Active-Passive HA Edge Pair, No Core System

Active-Active HA Edge Pair, No Core System