



▶ Polycom® DMA™ 7000 System  
Operations Guide

---

## Trademark Information



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

All other trademarks are the property of their respective owners.



Java is a registered trademark of Oracle America, Inc., and/or its affiliates.

## Patent Information

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

## End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom DMA 7000 system end-user license agreement (EULA).

The EULA is included in the release notes document for your version, which is available on the Polycom Support page for the Polycom DMA 7000 system.

© 2011-2012 Polycom, Inc. All rights reserved.

Polycom, Inc.  
4750 Willow Road  
Pleasanton, CA 94588-2708  
USA

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

---

# Contents

<b>1</b>	<b>Polycom® DMA™ 7000 System Overview</b>	<b>1</b>
	Introduction to the Polycom DMA System	1
	Polycom Solution Support	5
	Working in the Polycom DMA System	5
	Third-Party Software	9
	Open Source Software	9
<b>2</b>	<b>Polycom® DMA™ System Initial Configuration Summary</b>	<b>17</b>
	Add Required DNS Records for the Polycom DMA System	18
	License the Polycom DMA System	19
	Set Up Signaling	20
	Configure the Call Server	20
	Set Up Security	21
	Set Up MCUs	22
	Connect to Microsoft Active Directory	23
	Set Up Conference Templates	24
	Test the System	25
<b>3</b>	<b>System Security</b>	<b>27</b>
	Security Certificates Overview	27
	How Certificates Work	27
	Forms of Certificates Accepted by the Polycom DMA System	28
	How Certificates Are Used by the Polycom DMA System	29
	Frequently Asked Questions	30
	Certificate Settings	31
	Certificate Information Dialog Box	32
	Certificate Signing Request Dialog Box	33
	Add Certificates Dialog Box	33
	Certificate Details Dialog Box	34
	Certificate Procedures	35
	Install a Certificate Authority's Certificate	35

Create a Certificate Signing Request in the DMA System .....	36
Install a Certificate in the DMA System .....	38
Remove a Certificate from the DMA System .....	39
Security Settings .....	41
The Consequences of Enabling Maximum Security Mode .....	45
Login Policy Settings .....	48
Local Password .....	48
Session .....	49
Local User Account .....	50
Banner .....	51
Reset System Passwords .....	52
<b>4 Local Cluster Configuration .....</b>	<b>53</b>
Network Settings .....	54
Routing Configuration Dialog Box .....	57
Time Settings .....	58
Licenses .....	59
Signaling Settings .....	60
Logging Settings .....	63
Local Cluster Configuration Procedures .....	64
Add Licenses .....	64
Configure Signaling .....	66
Configure Logging .....	67
<b>5 Device Management .....</b>	<b>69</b>
Active Calls .....	69
Call Details Dialog Box .....	71
Endpoints .....	73
Add Device Dialog Box .....	78
Edit Device Dialog Box .....	78
Add Alias Dialog Box .....	80
Edit Alias Dialog Box .....	80
Associate User Dialog Box .....	80
Site Statistics .....	81
Site Link Statistics .....	82
External Gatekeeper .....	82
Add External Gatekeeper Dialog Box .....	84
Edit External Gatekeeper Dialog Box .....	86
External SIP Peer .....	88
Add External SIP Peer Dialog Box .....	89

Edit External SIP Peer Dialog Box .....	94
SIP Peer Postliminary Output Format Options .....	99
Add Authentication Dialog Box .....	103
Edit Authentication Dialog Box .....	103
Add Outbound Registration Dialog Box .....	104
Edit Outbound Registration Dialog Box .....	105
External SBC .....	106
Add External SBC Dialog Box .....	108
Edit External SBC Dialog Box .....	109
<b>6 MCU Management .....</b>	<b>111</b>
MCUs .....	111
Add MCU Dialog Box .....	117
Edit MCU Dialog Box .....	120
Add Session Profile Dialog Box .....	123
Edit Session Profile Dialog Box .....	123
MCU Procedures .....	124
MCU Pools .....	127
Add MCU Pool Dialog Box .....	128
Edit MCU Pool Dialog Box .....	129
MCU Pool Procedures .....	129
MCU Pool Orders .....	130
Add MCU Pool Order Dialog Box .....	132
Edit MCU Pool Order Dialog Box .....	133
MCU Pool Order Procedures .....	133
<b>7 Integrations with Other Systems .....</b>	<b>135</b>
Microsoft Active Directory Integration .....	135
Microsoft Active Directory Page .....	137
Active Directory Integration Procedure .....	141
Understanding Base DN .....	145
Adding Passcodes for Enterprise Users .....	146
About the System's Directory Queries .....	148
Microsoft Exchange Server Integration .....	153
Microsoft Exchange Server Page .....	155
Exchange Server Integration Procedure .....	155
Polycom CMA System Integration .....	157
Polycom CMA System Page .....	158
Join CMA Dialog Box .....	159
Polycom CMA System Integration Procedures .....	160

	Juniper Networks SRC Integration .....	161
	Juniper Networks SRC Page .....	161
	Juniper Networks SRC Integration Procedure .....	162
<b>8</b>	<b>Conference Manager Configuration .....</b>	<b>163</b>
	Conference Settings .....	163
	Conference Templates .....	165
	Two Types of Templates .....	165
	Template Priority .....	167
	About Conference IVR Services .....	167
	About Cascading .....	168
	Conference Templates List .....	169
	Add Conference Template Dialog Box .....	170
	Edit Conference Template Dialog Box .....	179
	Select Layout Dialog Box .....	187
	Conference Templates Procedures .....	188
	Shared Number Dialing .....	190
	Add Virtual Entry Queue Dialog Box .....	191
	Add Direct Dial Virtual Entry Queue Dialog Box .....	192
	Edit Virtual Entry Queue Dialog Box .....	193
	Edit Direct Dial Virtual Entry Queue Dialog Box .....	193
<b>9</b>	<b>Superclustering .....</b>	<b>195</b>
	About Superclustering .....	195
	DMAs .....	196
	Join Supercluster Dialog Box .....	199
	Supercluster Procedures .....	200
<b>10</b>	<b>Call Server Configuration .....</b>	<b>203</b>
	About the Call Server Capabilities .....	203
	Call Server Settings .....	205
	Domains .....	207
	Dial Rules .....	208
	The Default Dial Plan and Suggestions for Modifications .....	209
	Add Dial Rule Dialog Box .....	212
	Edit Dial Rule Dialog Box .....	214
	Script Debugging Dialog Box for Preliminaries/Postliminaries ....	215
	Sample Preliminary and Postliminary Scripts .....	216
	Hunt Groups .....	220

Add Hunt Group Dialog Box .....	221
Edit Hunt Group Dialog Box .....	221
Add Alias Dialog Box .....	222
Edit Alias Dialog Box .....	223
Device Authentication .....	223
Add Device Authentication Dialog Box .....	226
Edit Device Authentication Dialog Box .....	226
Registration Policy .....	227
Registration Policy Scripting .....	229
Script Debugging Dialog Box for Registration Policy Scripts .....	231
Sample Registration Policy Scripts .....	231
Prefix Service .....	234
Add Simplified Gateway Dialing Prefix Dialog Box .....	235
Edit Simplified Gateway Dialing Prefix Dialog Box .....	235
Embedded DNS .....	236
History Retention Settings .....	238
<b>11 Site Topology .....</b>	<b>241</b>
About Site Topology .....	241
Sites .....	243
Site Information Dialog Box .....	244
Add Site Dialog Box .....	244
Edit Site Dialog Box .....	248
Add Subnet Dialog Box .....	253
Edit Subnet Dialog Box .....	253
Site Links .....	254
Add Site Link Dialog Box .....	255
Edit Site Link Dialog Box .....	255
Site-to-Site Exclusions .....	256
Add Site-to-Site Exclusion Wizard .....	257
Territories .....	257
Add Territory Dialog Box .....	259
Edit Territory Dialog Box .....	260
Network Clouds .....	261
Add Network Cloud Dialog Box .....	261
Edit Network Cloud Dialog Box .....	262
Site Topology Configuration Procedures .....	263
<b>12 Users and Groups .....</b>	<b>265</b>
User Roles Overview .....	265

Adding Users Overview	267
Users	268
Add User Dialog Box	270
Edit User Dialog Box	272
Select Associated Endpoints Dialog Box	275
Conference Rooms Dialog Box	275
Add Conference Room Dialog Box	277
Edit Conference Room Dialog Box	279
Users Procedures	280
Conference Rooms Procedures	282
Groups	284
Import Enterprise Groups Dialog Box	285
Edit Group Dialog Box	286
Enterprise Groups Procedures	287
Login Sessions	289
Change Password Dialog Box	290
<b>13 System Management and Maintenance</b>	<b>291</b>
Management and Maintenance Overview	291
Administrator Responsibilities	292
Administrative Best Practices	292
Auditor Responsibilities	293
Auditor Best Practices	293
Recommended Regular Maintenance	293
Dashboard	296
Active Directory Integration Pane	297
Call Server Active Calls Pane	297
Call Server Registrations Pane	297
Cluster Info Pane	298
Conference History – Max Participants Pane	298
Conference Manager MCUs Pane	298
Conference Manager Usage Pane	299
Exchange Server Integration Pane	299
License Status Pane	300
Polycom CMA System Integration Pane	300
Supercluster Status Pane	301
Territory Status Pane	301
User Login History Pane	301
Alerts	302
Alert 1001	302



---

Alert 1002	302
Alert 1003	303
Alert 1004	303
Alert 1101	303
Alert 1102	303
Alert 1103	304
Alert 1104	304
Alert 2001	305
Alert 2002	305
Alert 2101	305
Alert 2102	306
Alert 2103	306
Alert 2104	306
Alert 2105	307
Alert 2106	307
Alert 2107	308
Alert 2201	308
Alert 2202	308
Alert 2203	309
Alert 3001	309
Alert 3101	309
Alert 3102	310
Alert 3103	310
Alert 3104	310
Alert 3105	311
Alert 3201	311
Alert 3202	311
Alert 3301	312
Alert 3302	312
Alert 3303	312
Alert 3304	312
Alert 3305	313
Alert 3401	313
Alert 3402	313
Alert 3403	314
Alert 3404	314
Alert 3405	314
Alert 3406	315
Alert 3601	315
Alert 3602	316

Alert 3603	316
Alert 3604	316
Alert 3605	316
Alert 3606	317
Alert 4001	317
Alert 4002	317
Alert 4003	317
Alert 5001	318
Alert 6001	318
Alert 7001	318
System Log Files	319
System Logs Procedures	320
Troubleshooting Utilities	322
Backing Up and Restoring	323
Backup and Restore Procedures	324
Upgrading the Software	328
Planning a Supercluster Upgrade	329
Upgrade Procedures	330
Adding a Second Server	333
Expanding an Unpatched System	334
Expanding a Patched System	335
Replacing a Failed Server	336
Shutting Down and Restarting	337

## **14 System Reports ..... 339**

Alert History	339
Call History	340
Export History	341
Conference History	341
Export History	342
Associated Calls	342
Conference Events	342
Property Changes	343
Call Detail Records (CDRs)	344
Exporting CDR Data	344
Call Record Layouts	344
Conference Record Layouts	346
Registration History Report	348
Registration History Procedures	349
Active Directory Integration Report	349

Orphaned Groups and Users Report .....	352
Orphaned Groups and Users Procedures .....	352
Conference Room Errors Report .....	353
Exporting Conference Room Errors Data .....	355
Enterprise Passcode Errors Report .....	355
Exporting Enterprise Passcode Errors Data .....	357
Network Usage Report .....	358
Exporting Network Usage Data .....	358
<b>Index .....</b>	<b>363</b>



---

# Polycom<sup>®</sup> DMA<sup>™</sup> 7000 System Overview

This chapter provides an overview of the Polycom<sup>®</sup> Distributed Media Application<sup>™</sup> (DMA<sup>™</sup>) 7000 system. It includes these topics:

- [Introduction to the Polycom DMA System](#)
- [Polycom Solution Support](#)
- [Working in the Polycom DMA System](#)
- [Third-Party Software](#)

## Introduction to the Polycom DMA System

The Polycom DMA system is a highly reliable and scalable video collaboration infrastructure solution based on the Polycom<sup>®</sup> Proxias<sup>™</sup> application server. It performs two primary functions and can be deployed in three configurations.

### Conference Manager Function

The Polycom DMA system's Conference Manager uses advanced routing policies to distribute voice and video calls among multiple media servers (Multipoint Control Units, or MCUs), creating a single virtual resource pool. This greatly simplifies video conferencing resource management and uses MCU resources more efficiently.

The Polycom DMA system integrates with your Microsoft<sup>®</sup> Active Directory<sup>®</sup>, automating the task of provisioning users for video conferencing. Combined with its advanced resource management, this makes reservationless video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.

The Polycom 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 re-provisioning.

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 Polycom DMA system distributes new conferences to the remaining MCUs. The consequences for existing calls and conferences depend on whether they're H.323 or SIP:

- H.323 calls and conferences on the failed MCU are terminated. But callers simply need to redial the same number they used for their initial dial-in. Conference Manager relocates their new conference to the best available MCU (provided there is still sufficient MCU capacity).
- SIP calls on the failed MCU are automatically moved to another MCU or MCUs (if available), up to the capacity available.

## Call Server Function

This version of the Polycom DMA system adds the Call Server to its feature set. The Call Server provides the following functionality:

- H.323 gatekeeper
- SIP registrar and proxy server
- H.323 <—> SIP gateway
- Bandwidth management

The Call Server can also be integrated with a Juniper Networks Service Resource Controller (SRC) to provide bandwidth assurance services.

## Two-server Cluster Configuration

The Polycom DMA system is designed to be deployed as a pair of co-located redundant servers that share the same virtual IP address(es). The two-server cluster configuration of the Polycom DMA system has no single point of failure within the system that could cause the service to become unavailable.

The two servers communicate over the private network connecting them. To determine which one should host the public virtual IP address, each server uses three criteria:

- Ability to ping its own public physical address
- Ability to ping the other server's public physical address
- Ability to ping the default gateway

In the event of a tie, the server already hosting the public virtual address wins.

Failover to the backup server takes about five seconds in the event of a graceful shutdown and about twenty seconds in the event of a power loss or other failure. In the event of a single server (node) failure, two things happen:

- All calls that are being routed through the failed server are terminated (including SIP calls, VMR calls, and routed mode H.323 calls). These users simply need to redial the same number, and they're placed back into conference. The standby server takes over the virtual signaling address, so existing registrations and new calls are unaffected.
- Direct mode H.323 point-to-point calls are not dropped, but the bandwidth management system loses track of them. This could result in overuse of the available network bandwidth.
- If the failed server is the active web host for the system management interface, the active user interface sessions end, the web host address automatically migrates to the remaining server, and it becomes the active web host. Administrative users can then log back into the system at the same URL. The system can always be administered via the same address, regardless of which server is the web host.

The internal databases within each Polycom DMA system server are fully replicated to the other node in the cluster. If a catastrophic failure of one of the database engines occurs, the system automatically switches itself over to use the database on the other server.

## Single-server Configuration

The Polycom DMA system is also available in a single-server configuration. This configuration offers all the advantages of the Polycom DMA system except the redundancy and fault tolerance at a lower price. It can be upgraded to a two-server cluster at any time.

This manual generally assumes a redundant two-server cluster. Where there are significant differences between the two configurations, those are spelled out.

## Superclustering

To provide geographic redundancy, up to five geographically distributed Polycom DMA system clusters (two-node 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 Polycom 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.

**Note**

Technically, a standalone Polycom DMA system (two-node or single-server) is a supercluster that contains one cluster. All the system configuration and other data that's shared across a supercluster is kept in the same data store. At any time, another Polycom DMA system can be integrated with it to create a two-cluster supercluster that shares its data store.

## System Capabilities and Constraints

The following capabilities and constraints apply to the entire supercluster:

- Number of sites: 500
- Number of clusters in a supercluster: 5 (not counting an integrated Polycom CMA system)
- Number of MCUs enabled for conference rooms: 64

The following capabilities and constraints apply to each cluster in the supercluster:

- Number of registrations: 15000
- Number of simultaneous H.323 calls: 5000
- Number of simultaneous SIP calls: 5000
- Total number of simultaneous calls: 5000
- Number of network usage data points retained: 8,000,000
- Number of IRQ messages sent per second: 100

## System Port Usage

Depending on signaling and security settings, the Polycom DMA system may have the following ports open:

- 22 – SSH (if Linux console access is enabled)
- 80 – redirects to 443
- 443 – redirects to 8443
- 8443 – management interface access
- 8444 – superclustering administration
- 4449 – OpenDS replication (superclustering)
- 5060 – unencrypted SIP (default port; can be changed)
- 5061 – SIP TLS (default port; can be changed)
- 1719 – RAS (default port; can be changed)
- 1720 – H.225 (default port; can be changed)



36000-61000 – H.245 port range

## Polycom Solution 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. These additional services will help customers successfully design, deploy, optimize, and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server or Lync Server 2010 integrations. For more information, please see [http://www.polycom.com/services/professional\\_services/index.html](http://www.polycom.com/services/professional_services/index.html) or contact your local Polycom representative.

## Working in the Polycom DMA System

This section includes some general information you should know when working in the Polycom DMA system.

### Field Input Requirements

While every effort was made to internationalize the Polycom 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.

### Settings Dialog Box

The **Settings** dialog box shows your user name and information about the server you're logged into. Click the  button to the right of the menus to display it.




In addition, you can change the text size used in the system interface and the maximum number of columns in the **Dashboard**. Note that larger text sizes will affect how much you can see in a given window or screen size and may require frequent scrolling.

## Polycom DMA System Management Interface Access

The Polycom DMA system has three system user roles that provide access to the management and operations interface. The functions you can perform and parts of the interface you can access depend on your user role or roles:

Menu/Icon	Admin	Provisioner	Auditor
 Home. Returns to the <a href="#">Dashboard</a> .	•	•	•
Network >			
Active Calls	•	•	
Endpoints	•	•	
DMA <sup>a</sup>	•	•	
MCU > MCU <sup>a</sup>	•	•	
MCU > MCU Pools <sup>a</sup>	•	•	
MCU > MCU Pool Orders <sup>a</sup>	•	•	
Site Statistics <sup>a</sup>	•	•	
Site Link Statistics <sup>a</sup>	•	•	
Site Topology > Sites <sup>a</sup>	•	•	
Site Topology > Site Links <sup>a</sup>	•	•	
Site Topology > Site-to-Site Exclusions <sup>a</sup>	•	•	
Site Topology > Network Clouds <sup>a</sup>	•	•	
Site Topology > Territories <sup>a</sup>	•	•	
External Gatekeeper <sup>a</sup>	•	•	
External SIP Peer <sup>a</sup>	•	•	
External SBC <sup>a</sup>	•	•	
User >			
Users <sup>b</sup>	•	•	
Groups	•		
Login Sessions <sup>a</sup>	•	•	
Change Password	•	•	•

Menu/Icon	Admin	Provisioner	Auditor
Reports >			
Call History	•	•	•
Conference History	•	•	•
Registration History	•	•	•
Network Usage	•	•	
Microsoft Active Directory Integration <sup>c</sup>	•		
Enterprise Passcode Errors <sup>c</sup>	•		
Orphaned Groups and Users	•	•	
Conference Room Errors <sup>c</sup>	•		
Maintenance			
System Log Files <sup>d</sup>	•		•
Troubleshooting Utilities > Ping, Traceroute, Top, I/O Stats, SAR	•		
Shutdown and Restart	•		
Software Upgrade	•		
Backup and Restore	•		
Admin > Conference Manager >			
Conference Settings	•		
Conference Templates	•		
Shared Number Dialing	•		
Admin > Call Server >			
Call Server Settings	•		
Domains	•		
Dial Rules	•		
Hunt Groups	•	•	
Device Authentication	•		
Registration Policy	•		
Prefix Service <sup>a</sup>	•	•	
Embedded DNS	•		
History Retention Settings	•		•

Menu/Icon	Admin	Provisioner	Auditor
Admin > Integrations >			
Microsoft Active Directory	•		
Microsoft Exchange Server	•		
Polycom CMA System	•		
Juniper Networks SRC	•		
Admin > Login Policy Settings >			
Local Password	•		
Session	•		
Local User Account	•		
Banner	•		
Admin > Local Cluster >			
Network Settings	•		
Signaling Settings	•		
Time Settings	•		
Licenses	•		
Logging Settings	•		•
Security Settings	•		
Certificates	•		
Help >			
About DMA 7000	•	•	•
Help Contents	•	•	•
 Settings. Displays Settings dialog box.	•	•	•
 Log Out. Logs you out of the Polycom DMA system.	•	•	•
 Help. Opens the online help topic for the page you're viewing.	•	•	•

- a. Provisioners have view-only access.
- b. Must be an enterprise user to see enterprise users. Provisioners can't add or remove roles or endpoints, and can't edit user accounts with explicitly assigned roles (Administrator, Provisioner, or Auditor), but can manage their conference rooms.
- c. Must be an enterprise user to view this report.
- d. Administrators can't delete log archives.

# Third-Party Software

## Open Source Software

The Polycom DMA system uses several open source software packages, including the CentOS operating system. CentOS is an enterprise-class Linux distribution that contains hundreds of open-source components. For more information about CentOS, visit <http://www.centos.org/>.

The packages containing the source code and the licenses for all the open-source software, including CentOS and its components, are included on the Polycom DMA system software DVD, mostly in the /SRPMS directory.

## Modifying Open Source Code

The LGPL v2.1 license allows you to modify the LGPL code we use, recompile the modified code, and re-link it with our proprietary code.

### Caution

Although you're free to modify the LGPL modules used in the Polycom DMA system, any changes you make may impair the system. If you modify any of the software, we can no longer provide support for your system.

### To replace an LGPL library with your modified version

- 1 On the DMA DVD, find the source code for the module you want to modify.
- 2 Modify the source code and compile it.
- 3 Go to **Configuration > System > Security Settings**, select **Allow Linux console access**, and click **Update**.
- 4 Contact Polycom Global Services for the root password for the Polycom DMA server.
- 5 Use ssh to log into the server as root.
- 6 Upload the modified software via wget or scp.
- 7 Find the module you're replacing and install the new version to that location.
- 8 Reboot the system.

## License Information

The following table contains license information for the open source software packages used in the Polycom DMA system. Note that the source code and the licenses for all the open-source software, including CentOS and its components, are included on the Polycom DMA system software DVD. This list is provided as a convenient reference.

Software	Version	License	Link
Axis	1.4.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
bsf	2.3.0-rc1	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
CentOs	5.6	GPLv2	<a href="https://www.redhat.com/licenses/gpl.html">https://www.redhat.com/licenses/gpl.html</a>
Cluster-glue	1.0.5	GPLv2	<a href="http://www.gnu.org/licenses/old-licenses/gpl-2.0.html">http://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
commons-beanutils	1.7	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-collections	3.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-configuration	1.5	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-digester	1.6	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-discovery	0.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-fileupload	1.2.1	Apache License, Version 2	<a href="http://commons.apache.org/fileupload/license.html">http://commons.apache.org/fileupload/license.html</a>
commons-httpclient	3.0.1	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-io	1.4	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-jexl	1.0	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-jxpath	1.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-lang	2.3	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-logging	1.0.4	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>

Software	Version	License	Link
commons-pool	1.3	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
corosync	1.2.5	BSD	<a href="http://opensource.org/licenses/bsd-license.php">http://opensource.org/licenses/bsd-license.php</a>
dom4j	1.5.2	BSD-style	<a href="http://www.dom4j.org/license.html">http://www.dom4j.org/license.html</a>
drools	4.0.0	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
Hibernate Annotations	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Hibernate (core)	3.2.4 SP 1	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Hsqldb	2.0.1-rc1	BSD-style	<a href="http://hsqldb.org/web/hsqLicense.html">http://hsqldb.org/web/hsqLicense.html</a>
JAF	1.1	Sun	<a href="http://download.oracle.com/otn-pub/java/licenses/jaf-1.1-fr-oth-JPR_license_1.html">http://download.oracle.com/otn-pub/java/licenses/jaf-1.1-fr-oth-JPR_license_1.html</a>
jamon	2.2	BSD-style	<a href="http://jamonapi.sourceforge.net/#JAMonLicense">http://jamonapi.sourceforge.net/#JAMonLicense</a>
Java JRE	1.6.0.20	Sun Microsystems, Binary Code license (BCL)	<a href="http://www.java.com/en/download/license.jsp">http://www.java.com/en/download/license.jsp</a>
JavaMail	1.4	Sun	<a href="http://download.oracle.com/otn-pub/java/licenses/javamail-1.4-oth-JPR_license_1.html">http://download.oracle.com/otn-pub/java/licenses/javamail-1.4-oth-JPR_license_1.html</a>
JBOSS AS	4.2.1 GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-aop	1.5.5	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-cache	1.4.1.sp14	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-jaxws	2.0.0.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-jmx	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-remoting	2.2.2.sp1	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-serialization	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jgroups	2.4.8.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
jcifs	1.3.2	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
jna	3.0.9 b0	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
joesnmp	0.3.4	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
libesmtplib	1.0.4	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
libnet	1.1.4		

Software	Version	License	Link
libxml2	1.2.3	MIT License	<a href="http://www.opensource.org/licenses/mit-license.html">http://www.opensource.org/licenses/mit-license.html</a>
Log4j	1.2.14	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
NSS	Part of Centos distrib.	Mozilla Public License v1.1	<a href="http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1">http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1</a>
NSS Tools	Part of Centos distrib.	Mozilla Public License v1.1	<a href="http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1">http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1</a>
NTP	Part of Centos distrib.	Open Software License v3.0	<a href="http://www.opensource.org/licenses/ntp-license.php">http://www.opensource.org/licenses/ntp-license.php</a>
OpenDS	2.2.0	CDDL	<a href="http://www.opensource.org/licenses/cddl1.php">http://www.opensource.org/licenses/cddl1.php</a>
openSSH	Part of Centos distrib.	OpenSSH	<a href="http://www.openssh.org">http://www.openssh.org</a>
openSSL	Part of Centos distrib.	OpenSSL	<a href="http://www.openssl.org/source/license.html">http://www.openssl.org/source/license.html</a>
Python	Part of Centos distrib.	Python Software Foundation License Version 2	<a href="http://python.org/download/releases/2.6.2/license">http://python.org/download/releases/2.6.2/license</a>
Quartz	1.5.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
Snmp4j	1.10.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
sudo	1.7.2p1	ISCL	<a href="https://www.isc.org/software/license">https://www.isc.org/software/license</a>
Xerces2	See JBoss.	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
OpenFire		Apache License, Version 2	<a href="http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html">http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html</a>
Rhino		Mozilla Public License, v1.1	<a href="http://www.mozilla.org/MPL/MPL-1.1.html">http://www.mozilla.org/MPL/MPL-1.1.html</a> AND <a href="https://developer.mozilla.org/en/Rhino_License">https://developer.mozilla.org/en/Rhino_License</a>
Web App Solution, Inc. Flex 3 dashboard		Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License, with a Creative Commons Plus License for commercial rights to the work.	<a href="http://creativecommons.org/licenses/by-nc-sa/3.0/">http://creativecommons.org/licenses/by-nc-sa/3.0/</a> <a href="http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html">http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html</a>



Software	Version	License	Link
The Open Source packages below are included in the Polycom DMA system as a consequence of being embedded in the Java Platform, Standard Edition Embedded, version 6.0. License text is available at <a href="http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT">http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT</a>			
CS CodeViewer	v1.0	BSD-like	
Crimson	v1.1.1	Apache 1.1	
Xalan J2		Apache 2.0	
NSIS	1.0j	(see license file)	
IAIK PKCS Wrapper		BSD-like	
Document Object Model (DOM)	v. Level 3	W3C SOFTWARE NOTICE AND LICENSE	
Xalan, Xerces		Apache 1.1	
W3C XML Conformance Test Suites	v. 20020606	W3C SOFTWARE NOTICE AND LICENSE	
W3C XML Schema Test Collection	v. 1.16.2	W3C SOFTWARE NOTICE AND LICENSE	
Mesa 3-D graphics library	v. 5	The core Mesa library is licensed according to the terms of the XFree86copyright (an MIT-style license). The Mesa source code is licensed under SGI FREE SOFTWARE LICENSE B (Version 1.1 [02/22/2000])	
Byte Code Engineering Library (BCEL)	v. 5	Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
CUP Parser Generator for Java	v. 0.10k	(general permissive license)	

Software	Version	License	Link
JLex Lexical Analyzer Generator for Java	v. 1.2.5	(general permissive license)	
SAX	v. 2.0.1	Public Domain	
Cryptix		Cryptix General License	
W3C XML Schema Test Collection		W3C DOCUMENT NOTICE AND LICENSE	
Stax API		BEA License (unique terms)	
X Window System		(general permissive license)	
dom4j	v. 1.6	BSD-like	
Retroweaver		(general permissive license)	
Stripper		BSD-like	
libpng official PNG reference library		(general permissive license)	
Libungif - An uncompressed GIF library		(general permissive license)	
Ant		Apache 2.0	
XML Resolver Library		Apache 2.0	
ICU4J		ICU License	
NekoHTML		Apache-like (1.1)	
Jing		(general permissive)	
RelaxNGCC		(general permissive)	
RELAX NG Object Model/ Parser		MIT License	
XFree86-VidMode Extension		Version 1.1 of Project Licence (BSD-like)	

Software	Version	License	Link
RelaxNGCC		version 2003-May-08 of the Info-ZIP copyright and license	<a href="ftp://ftp.info-zip.org/pub/infozip/license.html">ftp://ftp.info-zip.org/pub/infozip/license.html</a>
XML Security		Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
Zlib		(general permissive)	
Mozilla Rhino		Netscape Public License Version 1.1	
Apache Derby		Apache 2.0	
7-Zip		See file. Some files are LGPLv2.1; some have unRAR restriction; some are licensed under AES code license.	
UPX		GPL	
LZMA Software Development Kit		Common Public License (CPL)	



---

# Polycom<sup>®</sup> DMA<sup>™</sup> System Initial Configuration Summary

This chapter describes the configuration tasks required to complete your implementation of a new Polycom<sup>®</sup> Distributed Media Application<sup>™</sup> (DMA<sup>™</sup>) 7000 system once installation and initial network configuration are complete.

This chapter assumes you've completed the server configuration procedure in the *Getting Started Guide* (available at [support.polycom.com](http://support.polycom.com)), logged into the Polycom DMA system's management interface, and verified that the **Supercluster Status** pane of the **Dashboard** shows (for a two-server configuration) two servers in the cluster, with healthy enterprise and private network status for both.

Initial configuration includes the following topics:

## System configuration

- [Add Required DNS Records for the Polycom DMA System](#)
- [License the Polycom DMA System](#)
- [Set Up Signaling](#)
- [Configure the Call Server](#)
- [Set Up Security](#)
- [Set Up MCUs](#)
- [Connect to Microsoft Active Directory](#)
- [Set Up Conference Templates](#)

## Confirming configuration

- [Test the System](#)

Each topic describes the task, provides background and overview information for it, and where appropriate, links to specific step-by-step procedures to follow in order to complete the task.

**Note**

These topics outline the configuration tasks that are generally required. You may wish to complete other optional configuration tasks, including:

- Enable cascading of conferences (see [“About Cascading”](#) on page 168).
- Configure calendaring service ([“Microsoft Exchange Server Integration”](#) on page 153).

## Add Required DNS Records for the Polycom DMA System

In order to access your Polycom DMA system by its host name instead of by IP address, you (or your DNS administrator) must first create an A (*alias*) record (for IPv4) and/or AAAA record (for IPv6) on your DNS server(s).

For a two-server cluster configuration, at a minimum, create a record for the virtual host name and IP address shared by the two servers in the cluster. We recommend that you also create alias records for the two servers’ physical host names and IP addresses. For a superclustered system, A/AAAA records for each physical host name, physical IP address, and virtual host name are mandatory.

**Note**

Depending on local DNS configuration, the host name could be the Polycom DMA system’s fully qualified domain name (FQDN) or a shorter name that DNS can resolve. For some features, such as Microsoft Exchange Server integration, it’s imperative that the virtual host’s FQDN can be resolved in DNS, especially by the Exchange server.

If you’re using split network interfaces, we recommend creating alias records for both the management and signaling host names and addresses, but the signaling is the most important.

The DNS server(s) should also have entries for your Active Directory server (if different from the DNS server) and external gatekeeper (if using legacy signaling mode).

If you’re going to use the Call Server functionality (instead of legacy signaling mode), you may want to create additional DNS records as described below.

### Additional DNS Records for SIP Proxy

To support the use of your Polycom DMA system as a SIP proxy server, you may want to create the following DNS records (for each cluster in a supercluster, if applicable):

- NAPTR records, which describe the transport protocols that are supported by the SIP proxies at a domain. Configure these statically to match the system’s SIP transport protocol configuration.

- SRV records, which 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.

For more information about the use of DNS in SIP, refer to RFC 3263.

### Additional DNS Records for H.323 Gatekeeper

To support the use of your Polycom DMA system as an H.323 gatekeeper, you may want to create SRV records, which identify the host names of the gatekeepers that service a particular domain. These records are necessary in order to enable the optional inbound URL dialing feature. Configure them statically to point to the host names of the Call Servers in the domain.

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.

### Additional DNS Records for the Optional Embedded DNS Feature

To support DNS publishing by your Polycom DMA system's embedded DNS servers (see "Embedded DNS" on page 236), a DNS NS record is needed for each cluster in the supercluster. These records identify the Polycom DMA system's embedded DNS servers as authoritative for the specified logical host names. Here are two example records:

```
callservers-<site name>.example.com. 86400 IN NS dma1.example.com.  
callservers-<site name>.example.com. 86400 IN NS dma2.example.com.
```

## License the Polycom DMA System

The Polycom DMA system license you purchased specifies how many concurrent calls it can handle. You should have received either one or two license numbers, depending on whether you ordered a single-server system or a two-server cluster.

You must obtain an activation key code for each server from the Polycom Resource Center (PRC). You enter the server's serial number and the license number that you were given for that server, and the PRC generates an activation key for that server. For a cluster, you repeat the process using the other server's serial number and its license number. Installing the activation keys activates the licenses for your system.

#### Caution

An activation key is linked to a specific server's serial number. For a two-server cluster, you must generate the activation key for each server using that server's serial number. Licensing will fail if you generate both activation keys from the same server serial number.

To activate the system license, follow the procedure in [“Licenses”](#) on page 59.

## Set Up Signaling

Signaling setup includes enabling H.323, SIP, or both, and optionally setting the prefix for dialing into the system.

### Note

The addition of the Call Server and superclustering features to the Polycom DMA system required significant changes to the signaling internals. One consequence of these changes is that the Polycom DMA system can no longer register to an external gatekeeper as an MCU. Instead, it can neighbor to an external gatekeeper as another gatekeeper. As a result, if you're upgrading from a version that didn't include the Call Server functionality or that operated in what was known as “legacy signaling mode,” you need to reconfigure your external gatekeeper.

To configure signaling, follow the procedure in [“Configure Signaling”](#) on page 66.

## Configure the Call Server

Configuring the Polycom DMA system's Call Server function consists of the following high-level tasks:

- 1 Integrate with a Polycom CMA system (see [“Polycom CMA System Integration”](#) on page 157) or enter site topology information (see [“Site Topology”](#) on page 241).
- 2 If deploying a supercluster of multiple geographically distributed Polycom DMA clusters:
  - a Set the **Security Configuration** page security options before superclustering (see [“Security Settings”](#) on page 41). But wait until after superclustering to do the rest of the security setup tasks.
  - b Depending on the security settings, you may need to install certificates before superclustering (see [“Certificate Procedures”](#) on page 35).
  - c Create a supercluster (see [“About Superclustering”](#) on page 195) and configure supercluster options.
- 3 Create territories and assign sites to them. Assign the primary and backup cluster responsible for each territory, and designate which territories can host conference rooms (see [“Territories”](#) on page 257).
- 4 Add any external devices, such as a neighbor gatekeeper or SIP peer (see [“Call Server Configuration”](#) on page 203).



- 5 Configure the dial plan (see [“Dial Rules”](#) on page 208).

## Set Up Security

The first step in securing your Polycom DMA system is to locate it in a secure data center with controlled access, but that topic is beyond the scope of this document.

Secure setup of the Polycom DMA system consists of the following high-level tasks (some of which assume you’re integrating with Active Directory and some of which overlap with subsequent initial setup topics):

- 1 As the default local administrative user (admin), create a local user account for yourself with the Administrator role, log in using that account, and delete the admin user account. See [“Adding Users Overview”](#) on page 267 and [“Users Procedures”](#) on page 280.
- 2 Create the service account (read-only user account) that the Polycom DMA system will use to read and integrate with Active Directory. See [“Active Directory Integration Procedure”](#) on page 141.
- 3 Assign the Administrator role to your named enterprise account, and remove the Polycom DMA system’s user roles (see [“User Roles Overview”](#) on page 265) from the service account used to integrate with Active Directory. See [“Connect to Microsoft Active Directory”](#) on page 23 and [“Microsoft Active Directory Integration”](#) on page 135.
- 4 Log out and log back in using your enterprise user ID and password.
- 5 Verify that the expected enterprise users are available in the Polycom DMA system and that conference room IDs were successfully created for them. If necessary, adjust integration settings and correct errors. See [“Microsoft Active Directory Integration”](#) on page 135, [“Users Procedures”](#) on page 280, and [“Conference Room Errors Report”](#) on page 353.
- 6 Obtain and install a security certificate from a trusted certificate authority. See [“Security Certificates Overview”](#) on page 27 and [“Certificate Procedures”](#) on page 35.
- 7 Document your current configuration for comparison in the future. We recommend saving screen captures of all the configuration pages.
- 8 Manually create a backup, download it, and store it in a safe place. See [“Backing Up and Restoring”](#) on page 323.

## Set Up MCUs

### Note

The Polycom DMA system can interact with MCUs, or media servers, in either or both of the following two ways:

- MCUs may be made available to system's Conference Manager to manage for multi-point conferencing (hosting virtual meeting rooms, or VMRs).
- MCUs may be registered with the system's Call Server as standalone MCUs and/or gateways.

This configuration summary assumes you want to do both.

Make sure your RMX MCUs are configured to accept encrypted (HTTPS) management connections (required for maximum security mode).

Make sure that each MCU is in a site belonging to a territory for which the Polycom DMA system is responsible. If you're deploying a supercluster (see ["Configure the Call Server"](#) on page 20 and ["About Superclustering"](#) on page 195), make sure that each territory has a primary and backup cluster assigned to it. If the primary cluster becomes unavailable, the MCUs registered to it can re-register to the backup.

If you're deploying a supercluster, verify that you've enabled the hosting of conference rooms in the right territories and assigned clusters to those territories. See ["Configure the Call Server"](#) on page 20.

Standalone MCUs can register themselves to the Polycom DMA system's Call Server. To make an MCU available as a conferencing resource, either add it to the appropriate Polycom DMA cluster's Conference Manager manually or, if it's already registered with the Call Server, edit its entry to enable it for conference rooms and provide the additional configuration information required. See ["MCU Management"](#) on page 111.

You must organize MCUs configured as conferencing resources into one or more MCU pools (logical groupings of media servers). Then, you can define one or more MCU pool orders that specify the order of preference in which MCU pools are used.

Every conference room (VMR) is associated with an MCU pool order. 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. See ["MCU Pools"](#) on page 127 and ["MCU Pool Orders"](#) on page 130 for information about how to use pools and pool orders, as well as the rules that the system uses to choose an MCU for a user.

The Polycom DMA system uses conference templates to define the conferencing experience associated with a conference room or enterprise group. You can create standalone templates (recommended), setting the conferencing parameters directly in the Polycom DMA system, or link templates to RMX conference profiles (see ["Conference Templates"](#) on page 165).

Both methods allow you to specify most conference parameters:

- General information such as line rate, encryption, auto termination, and H.239 settings
- Video settings such as mode (presentation or lecture) and layout
- IVR settings
- Conference recording settings

If you want to create DMA system templates linked to conference profiles on the RMX MCUs, make sure the profiles used by the Polycom DMA system exist on all the RMX MCUs and are defined the same on all of them.

## Connect to Microsoft Active Directory

Connecting to Microsoft® Active Directory® simplifies the task of deploying conferencing to a large organization. All Polycom DMA system access to the Active Directory server is read-only and minimally impacts the directory performance. See [“Microsoft Active Directory Integration”](#) on page 135.

### Note

If you're not knowledgeable about enterprise directories in general and your specific implementation in particular, please consult with someone who is. Active Directory integration is a non-trivial matter.

Before integrating with Active Directory, be sure that one or more DNS servers are specified (this should have been done during installation and initial setup). See [“Network Settings”](#) on page 54.

If you're deploying a supercluster of multiple geographically distributed Polycom DMA clusters, verify that you've assigned clusters to the territories in your site topology (see [“Configure the Call Server”](#) on page 20) and decide which cluster is to be responsible for Active Directory integration.

Active Directory integration automatically makes the enterprise users (directory members) into Conferencing Users in the Polycom DMA system, and can assign each of them a conference room (virtual meeting room). The conference room IDs are typically generated from the enterprise users' phone numbers.

### Note

Creating conference rooms (virtual meeting rooms, or VMRs) for enterprise users is optional. If you want to integrate with Active Directory to load user and group information into the Polycom DMA system, but don't want to give all users the ability to host conferences, you can do so. You can manually add conference rooms for selected users at any time. See [“Conference Rooms Procedures”](#) on page 282.

Once the Polycom DMA system is integrated with Active Directory, it reads the directory information nightly, so that user and group information is updated automatically as people join and leave the organization. The system caches the data from Active Directory. In a superclustered system, one cluster is responsible for updating the cache, which is shared with all the clusters.

Between updates, clusters access the directory only to authenticate passwords; all other user information (such as user search results) comes from the cache. You can manually update the cache at any time.

Enterprise groups can have their own conference templates that provide a custom conferencing experience (see [“Conference Templates”](#) on page 165). They can also have their own MCU pool order, which preferentially routes conferences to certain MCUs (see [“MCU Pool Orders”](#) on page 130).

You can assign Polycom DMA system roles to an enterprise group, applying the roles to all members of the group and enabling them to log into the Polycom DMA system’s management interface with their standard network user names and passwords.

See [“User Roles Overview”](#) on page 265, [“Groups”](#) on page 284, and [“Enterprise Groups Procedures”](#) on page 287.

There are security concerns that need to be addressed regarding user accounts, whether local or enterprise. See the high-level process described in [“Set Up Security”](#) on page 21.

## Set Up Conference Templates

The Polycom DMA system uses conference templates and global conference settings to manage system and conference behavior, and it has a default conference template and default global conference settings.

After you’ve added MCUs to the system, you may want to change the global conference settings or create additional templates that specify different conference properties.

If you integrate with Active Directory, you can use templates to provide customized conferencing experiences for various enterprise groups.

When you add a custom conference room to a user (either local or enterprise), you can choose which template that conference room uses.

To add conference templates, see [“Conference Templates Procedures”](#) on page 188. To change conference settings, see [“Conference Settings”](#) on page 163. To customize the conferencing experience for an enterprise group, see [“Enterprise Groups Procedures”](#) on page 287.

## Test the System

On the **Signaling Settings** page (see [“Signaling Settings”](#) on page 60), verify that:

- If you enabled H.323, the **H.323 Signaling Status** section indicates that the signaling status is **Active** and the port assignments are correct.
- If you enabled SIP, the **SIP Signaling Status** section shows that the correct protocols and listening ports are enabled.

Have some endpoints register with the Polycom DMA Call Server and make point-to-point calls to each other.

On the **Dashboard** (see [“Dashboard”](#) on page 296), verify that:

- The information in the **Cluster Info** pane looks correct, including the time, network settings, and system resource information.
- The **Supercluster Status** pane shows the correct number of servers and clusters, and the network interfaces that should be working (depending on your IP type and split network settings) are up (green up arrow) and in full duplex mode, with the speed correct for your enterprise network.
- The **Call Server Registrations** pane shows that the endpoints that attempted to register did so successfully.
- The **Call Server Active Calls** pane shows that the endpoints that made calls did so successfully, and the call limits per cluster and total are correct for your licenses.
- The **Conference Manager MCUs** pane shows that the MCUs you added are connected and in service.
- The information on the **Active Directory Integration** pane looks correct, including the status, cache refresh data, and enterprise conference room count.

Set up some multipoint conferences by having endpoints dial into enterprise users' conference rooms (preferably including a custom conference room). Verify that conferencing works satisfactorily, that the system status is good, and that the **Conference Manager Usage** pane accurately presents the status.

When you're satisfied that the Polycom DMA system is configured and working properly, manually create a backup, download it, and store it in a safe place. See [“Backing Up and Restoring”](#) on page 323.



---

# System Security

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system security topics:

- [Security Certificates Overview](#)
- [Certificate Settings](#)
- [Certificate Procedures](#)
- [Security Settings](#)
- [The Consequences of Enabling Maximum Security Mode](#)
- [Login Policy Settings](#)
- [Reset System Passwords](#)

## Security Certificates Overview

### How Certificates Work

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other.

- A single, centralized certificate authority (CA) is established. Typically, this is either an enterprise's IT department or a commercial certificate authority.
- Each computer on the network is configured to trust the central certificate authority.
- Each server on the network has a public certificate that identifies it.
- The certificate authority signs the public certificates of those servers that clients should trust.

- When a client connects to a server, the server shows its signed public certificate to the client. Trust is established because the certificate has been signed by the certificate authority, and the client has been configured to trust the certificate authority.

## Forms of Certificates Accepted by the Polycom DMA System

X.509 certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the Polycom DMA system.

Encoding	Protocol / File Type	Description and Installation Method
PEM (Base64-encoded ASCII text)	PKCS #7 protocol P7B file	Certificate chain containing: <ul style="list-style-type: none"> <li>• A signed certificate for the system, authenticating its public key.</li> <li>• The CA's public certificate.</li> <li>• Sometimes intermediate certificates.</li> </ul> Upload file or paste into text box.
	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.
DER (binary format using ASN.1 Distinguished Encoding Rules)	PKCS #12 protocol PFX file	Certificate chain containing: <ul style="list-style-type: none"> <li>• A signed certificate for the system, authenticating its public key.</li> <li>• A private key for the system.</li> <li>• The CA's public certificate.</li> </ul> Upload file.
	PKCS #7 protocol P7B file	Certificate chain containing: <ul style="list-style-type: none"> <li>• A signed certificate for the system, authenticating its public key.</li> <li>• The CA's public certificate.</li> <li>• Sometimes intermediate certificates.</li> </ul> Upload file.
	CER (single certificate) file	Signed certificate for the system, authenticating its public key. Upload file.



## How Certificates Are Used by the Polycom DMA System

The Polycom DMA system uses X.509 certificates in four different ways:

- 1 When a user logs into the Polycom DMA system's browser-based management interface, the Polycom DMA system (server) offers an X.509 certificate to identify itself to the browser (client).

The Polycom DMA system's certificate must have been signed by a certificate authority (see "[Certificate Procedures](#)" on page 35).

The browser must be configured to trust that certificate authority (beyond the scope of this documentation).

If trust can't be established, most browsers allow connection anyway, but display a 'nag' dialog to the user, requesting permission.

- 2 When the Polycom DMA system connects to a Microsoft Active Directory server, it may present a certificate to the server to identify itself.

If Active Directory is configured to require a client certificate (this is not the default), the Polycom 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.

- 3 When the Polycom DMA system connects to a Microsoft Exchange server (if the calendaring service is enabled; see "[Microsoft Exchange Server Integration](#)" on page 153), it may present a certificate to the server to identify itself.

Unless the **Allow unencrypted calendar notifications from Exchange server** security option is enabled (see "[Security Settings](#)" on page 41), the Polycom 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 (see "[Dashboard](#)" on page 296) remains **Subscription pending** indefinitely, the Polycom DMA system does not receive calendar notifications, and incoming meeting request messages are only processed approximately every 4 minutes.

- 4 When the Polycom DMA system connects to an RMX MCU configured for secure communications (this is not the default), a certificate may be used to identify the RMX MCU (server) to the Polycom DMA system (client).

## Frequently Asked Questions

**Q.** Is it secure to send my certificate request through email?

**A.** Yes. The certificate request, signed certificate, intermediate certificates, and authority certificates that are sent through email don't contain any secret information. There is no security risk in letting untrusted third parties see their contents.

As a precaution, you can verify the certificate fingerprints (which can be found in the Certificate Details popup) with the certificate authority via telephone. This ensures that a malicious third party didn't substitute a fake email message with fake certificates.

**Q.** Why doesn't the information on the Certificate Details popup match the information that I filled out in the signing request form?

**A.** Commercial certificate authorities routinely replace the organizational information in the certificate with their own slightly different description of your organization.

**Q.** I re-installed the Polycom DMA system software. Why can't I re-install my signed public certificate?

**A.** X.509 certificates use public/private key pair technology. The public key is contained in your public certificate and is provided to any web browser that asks for it. The private key never leaves the Polycom DMA system.

As part of software installation, the Polycom DMA system generates a new public/private key pair. The public key from your old key pair can't be used with the new private key.

To re-use your signed public certificate, try restoring from backup. Both the public and private keys are saved as part of a backup file.

See also:

["System Security"](#) on page 27

["Certificate Settings"](#) on page 31

["Certificate Procedures"](#) on page 35

## Certificate Settings

The following table describes the fields on the **Certificate Settings** page.

**Table 3-1** Fields on the Certificate Settings page

Column	Description
Enable OCSP	<p>Enables the use of Online Certificate Status Protocol as a means of obtaining the revocation status of a certificate presented to the system.</p> <p>If <b>OCSP responder URL</b> is not specified, the system checks the certificate's AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder:</p> <ul style="list-style-type: none"> <li>• If there is none, the certificate fails validation.</li> <li>• Otherwise, the system sends the OCSP request to the responder identified in the certificate.</li> </ul> <p>If <b>OCSP responder URL</b> 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.</p> <p>If <b>OCSP certificate</b> is specified, the response message must be signed by the specified certificate's private key.</p>
OCSP responder URL	<p>Identifies the responder to be used for all OCSP requests, overriding the AIA field values.</p> <p>If <b>OCSP certificate</b> is specified, the response message must be signed by the specified certificate's private key.</p>
OCSP certificate	<p>Select a certificate to require OCSP response messages to be signed by the specified certificate's private key.</p>
Store OCSP Configuration	<p>Saves the OCSP configuration.</p>
Identifier	<p>Common name of the certificate.</p>
Purpose	<p>Kind of certificate:</p> <ul style="list-style-type: none"> <li>• Server SSL is the system's public certificate, which it presents to identify itself. By default, this is a self-signed certificate, not trusted by other devices.</li> <li>• Trusted Root CA is the root certificate of a certificate authority that the DMA system trusts.</li> <li>• 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 DMA system trusts the root CA, then the chain consisting of it, its intermediate CA certificates, and the server certificate will all be trusted.</li> </ul>
Expiration	<p>Expiration date of certificate.</p>

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Information Dialog Box”](#) on page 32

[“Certificate Signing Request Dialog Box”](#) on page 33

[“Add Certificates Dialog Box”](#) on page 33

[“Certificate Details Dialog Box”](#) on page 34

[“Certificate Procedures”](#) on page 35

## Certificate Information Dialog Box

The **Certificate Information** dialog box appears when you click **Create Certificate Signing Request** in the **Actions** list (if a signing request has already been issued, you’re first asked whether to use the existing one or create a new one). The following table describes the fields in the dialog box.

**Table 3-2** *Fields in the Certificate Information dialog box*

Field	Description
Common name (CN)	Defaults to the FQDN of the system’s management interface, as defined by the virtual host name and domain specified on the <b>Network</b> page. Editable.
Organizational unit (OU)	Subdivision of organization. Specify up to three OUs. Optional.
Organization (O)	Optional.
City or locality (L)	Optional.
State (ST)	Optional.
Country (C)	Two-character country code.

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Certificate Signing Request Dialog Box

The **Certificate Signing Request** dialog box appears when you create a request in the **Certificate Information** dialog box.

The **Summary** section at the top displays the information the **Certificate Information** dialog box.

The **Encoded Request** box below displays the encoded certificate request text, which you can select and copy.

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Add Certificates Dialog Box

The **Add Certificates** dialog box appears when you click **Add Certificates** in the **Actions** list. It lets you install signed certificates or certificate chains. You can do so in two ways:

- Upload a PFX, PEM, or P7B certificate file.
- Paste PEM-format certificate text into the dialog box.

The following table describes the fields in the dialog box.

**Table 3-3** Fields in the Add Certificates dialog box

Field	Description
Upload certificate	If checked, the <b>Password</b> field and <b>Upload file</b> button enable you to upload a PFX, PEM, or P7B certificate file.
Password	Enter the password, if any, assigned to the certificate file when it was created.
Upload file	Click the button to browse to the file you want to upload.
Paste certificate	If checked, the text field below enables you to paste in the text of PEM certificate files.

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Certificate Details Dialog Box

The **Certificate Details** dialog box appears when you click **Display Details** in the **Actions** list. It displays information about the certificate selected in the list, as outlined in the following table.

**Table 3-4** Sections in the Certificate Details dialog box

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

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Certificate Procedures

Certificate procedures include the following:

- [Install your chosen certificate authority's public certificate](#), if necessary, so that the Polycom DMA system trusts that certificate authority.
- [Create a certificate signing request](#) to submit to the certificate authority.
- [Install a public certificate signed by your certificate authority](#) that identifies the Polycom DMA system.
- [Remove a signed certificate or a certificate authority's certificate](#).

### Note

If you're configuring the Polycom DMA system to support Polycom's solution for the Microsoft OCS or Lync 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).

Once you have the PFX file, you're ready to [install it](#).

See Polycom's solution deployment guide for information about using the Certificate Wizard and other steps needed to implement the solution.

## Install a Certificate Authority's Certificate

This procedure is not necessary if you obtain a certificate chain that includes a signed certificate for the Polycom 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 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 can't implement the change until it restarts and reads the changed certificate store.

For your convenience, you're not required to restart and apply a change immediately. This permits you to perform multiple installs or removals before restarting and applying the changes. But when you're finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Before you begin, make sure there are no active conferences and you're prepared to restart the system when you're finished.

### To install a certificate for a trusted root CA

- 1 Go to **Admin > Local Cluster > 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 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 box, 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**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.

See also:

["Security Certificates Overview"](#) on page 27

["Certificate Settings"](#) on page 31

["Certificate Procedures"](#) on page 35

## Create a Certificate Signing Request in the DMA System

The procedure below creates a certificate signing request (CSR) that you can submit to your chosen certificate authority.

### To create a certificate signing request

- 1 Go to **Admin > Local Cluster > 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 *Server SSL* certificate.





## Install a Certificate in the DMA System

The procedure below installs the certificate or certificate chain provided by the certificate authority. It assumes that you've received the certificate or certificate chain in one of the following forms:

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

### Caution

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 can't implement the change until it restarts and reads the changed certificate store.

For your convenience, you're not required to restart and apply a change immediately. This permits you to perform multiple installs or removals before restarting and applying the changes. But when you're finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Before you begin, make sure there are no active conferences and you're prepared to restart the system when you're finished.

### To install a signed certificate that identifies the Polycom DMA system

- 1 When you receive your certificate(s), return to **Admin > Local Cluster > Certificates**.
- 2 In the **Actions** list, select **Add Certificates**.
- 3 In the **Add Certificates** dialog box, 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 box appears.
  - c Confirm from the information under **Issued To** and **Issued By** that the self-signed default certificate has been replaced by your signed public certificate from the certificate authority.

- d** Click **OK** to close the dialog box.
- 6** Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Remove a Certificate from the DMA 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 as the Server SSL certificate so that the system reverts to using the default self-signed Server SSL certificate.

Removing a signed certificate also removes the certificate of the Trusted Root CA that signed it, along with any intermediate certificates provided by that certificate authority.

Both procedures are described below.

### Caution

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 can't implement the change until it restarts and reads the changed certificate store.

For your convenience, you're not required to restart and apply a change immediately. This permits you to perform multiple installs or removals before restarting and applying the changes. But when you're finished making changes, you must select **Restart to Apply Saved Changes** to restart the system and finish your update. Before you begin, make sure there are no active conferences and you're prepared to restart the system when you're finished.

### To remove a Trusted Root CA's certificate

- 1** Go to **Admin > Local Cluster > Certificates**.
- 2** In the certificates list, select the certificate you want to delete.
- 3** In the **Actions** list, select **Display Details** and confirm that you've selected the correct certificate. Then click **OK**.
- 4** In the **Actions** list, select **Delete Certificate**.

- 5 When asked to confirm, click **Yes**.  
A dialog box informs you that the certificate has been deleted.
- 6 Click **OK**.
- 7 Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.

### To remove a signed certificate and revert to the default self-signed certificate

- 1 Go to **Certificates**.
- 2 In the **Actions** list, select **Revert to Default Certificate**.
- 3 When asked to confirm, click **Yes**.  
A dialog box informs you that the system has reverted to a self-signed certificate.
- 4 Click **OK**.
- 5 Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.
- 6 After the system restarts, log back in, return to **Admin > Local Cluster > 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 In the **Actions** list, select **Display Details**.  
The **Certificate Details** dialog box appears.
  - c Confirm from the information under **Issued To** and **Issued By** that the default self-signed certificate has replaced the CA-signed certificate.
  - d Click **OK** to close the dialog box.

See also:

[“Security Certificates Overview”](#) on page 27

[“Certificate Settings”](#) on page 31

[“Certificate Procedures”](#) on page 35

## Security Settings

The **Security Settings** page lets you switch between high security mode and a custom security mode in which one or more insecure capabilities are allowed. It also lets you switch to, but not from, a maximum security mode.

### Caution

We recommend always using the **High security** setting unless you have a specific and compelling need to allow one of the insecure capabilities.

We recommend the new **Maximum security** setting only for those environments where the most stringent security protocols must be adhered to.

Enabling **Maximum security** is *irreversible* and has significant consequences (see “[The Consequences of Enabling Maximum Security Mode](#)” on page 45). Don't choose this setting unless you know what you're doing and are prepared for the consequences.

### Note

All clusters in a supercluster must have the same security settings. Before attempting to join a supercluster, make sure the cluster's security settings match those of the other members of the supercluster. You can't change a cluster's security settings while it's part of a supercluster.

The following table describes the options in the **Security Settings** page.

**Table 3-5** Fields on the Security Settings page

Field	Description
<b>Maximum security</b>	An extremely high security mode suitable for use where very strict security requirements apply. Once this mode is enabled, it's no longer possible to reduce the security level. See caution above.
<b>High security</b>	Recommended setting for normal operation.
<b>Custom security</b>	Lets you enable one or more of the unsecured methods of network access listed below it.
Allow Linux console access	Enables the Linux user root to log into the system using SSH. This direct Linux access isn't needed for normal operation, routine maintenance, or even troubleshooting, all of which can be done through the administrative GUI.  In extreme circumstances, this option might enable expert Polycom Global Services personnel to more fully understand the state of a troubled system or correct problems. Enable this option only when asked to do so by Polycom Global Services.

**Table 3-5** Fields on the Security Settings page (continued)

Field	Description
Allow unencrypted connections to the Active Directory	<p>Normally, the Polycom DMA system connects to Active Directory using SSL or TLS encryption. But if the Active Directory server or servers (including domain controllers if you import global groups) aren't configured to support encryption, the Polycom DMA system can only connect using an unencrypted protocol. This option allows such connections if an encrypted connection can't be established.</p> <p>This configuration causes an extreme security flaw: the unencrypted passwords of enterprise users are transmitted over the network, where they can easily be intercepted.</p> <p>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.</p>
Allow unencrypted connections to MCUs	<p>Normally, the Polycom DMA system uses only HTTPS for the conference control connection to RMX MCUs, and therefore can't control an RMX MCU that accepts only HTTP (the default). This option enables the system to fall back to HTTP for RMX MCUs not configured for HTTPS.</p> <p>We recommend configuring your MCUs to accept encrypted connections rather than enabling this option. When unencrypted connections are used, the RMX login name and password are sent unencrypted over the network.</p>
Allow unencrypted calendar notifications from Exchange server	<p>Normally, if calendaring is enabled, the Polycom DMA system gives the Microsoft Exchange server an HTTPS URL to which the Exchange server can deliver calendar notifications. In that case, the Polycom DMA system must have a certificate that the Exchange server accepts in order for the HTTPS connection to work.</p> <p>If this option is selected, the Polycom DMA system does not require HTTPS for calendar notifications.</p> <p>We recommend installing a certificate trusted by the Exchange server and using an HTTPS URL for notifications rather than enabling this option.</p>

**Table 3-5** Fields on the Security Settings page (continued)

Field	Description
Allow basic authentication to Exchange server	<p>Normally, if calendaring is enabled, the Polycom DMA system authenticates itself with the Exchange server using NTLM authentication.</p> <p>If this option is selected, the Polycom DMA system still attempts to use NTLM first. But if that fails or isn't enabled on the Exchange server, then the DMA system falls back to HTTP Basic authentication (user name and password).</p> <p>We recommend using NTLM authentication rather than enabling this option.</p> <p>In order for either NTLM or HTTP Basic authentication to work, they must be enabled on the Exchange server.</p>
Skip certificate validation for server connecting	<p>Normally, when the Polycom DMA system connects to a server, it validates that server's certificate.</p> <p>This option configures the system to accept any certificate presented to it without validating it.</p> <p>We recommend 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:</p> <ul style="list-style-type: none"> <li>MCUs</li> <li>Active Directory</li> <li>Exchange</li> <li>CMA system</li> <li>Other DMA systems</li> </ul>
Skip certificate validation for encrypted signaling	<p>Normally, during encrypted call signaling (SIP over TLS), the Polycom DMA system requires the remote party (endpoint or MCU) to present a valid certificate.</p> <p>This option configures the system to accept any certificate (or none).</p> <p>We recommend installing valid certificates on your endpoints and MCUs rather than enabling this option.</p>

**Table 3-5** Fields on the Security Settings page (continued)

Field	Description
Skip certificate validation for user login sessions	<p>Unlike the preceding settings, this option is compatible with the <b>High security</b> or <b>Maximum security</b> setting.</p> <p>If this option is turned off, you can only connect to the Polycom DMA system if your browser presents a client certificate issued by a CA that the system trusts.</p> <p>Turn this option off only if:</p> <ul style="list-style-type: none"> <li>You've 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.</li> <li>The CA's public certificate is installed in the Polycom DMA system so that it trusts the CA.</li> <li>All authorized users, including yourself, have a client certificate signed by the CA that authenticates them to the Polycom DMA system.</li> </ul>

**To change the security settings**

- 1 Go to **Admin > Local Cluster > Security Settings**.
- 2 To switch from a custom setting back to the recommended security mode, click **High security**.
- 3 To switch from the recommended security mode to a custom setting:
  - a Click **Custom security**.
  - b Check the unsecured network access method(s) that you want to enable.
- 4 Click **Update**.  
A dialog box informs you that the configuration has been updated.

**Note**

If you turn off **Skip certificate validation for user login sessions**, the system notifies you that if you don't log back in within 5 minutes, the setting will be automatically turned back on. This is a safety precaution to ensure that at least one user is still able to access the system.

- 5 Click **OK**.



See also:

[“System Security”](#) on page 27

[“Certificate Settings”](#) on page 31

[“The Consequences of Enabling Maximum Security Mode”](#) on page 45

[“Login Policy Settings”](#) on page 48

[“Reset System Passwords”](#) on page 52

## The Consequences of Enabling Maximum Security Mode

Enabling the **Maximum security** setting is irreversible and has the following significant consequences:

- All unencrypted protocols and unsecured access methods are disabled.
- The boot order is changed so that the server(s) can't be booted from the optical drive or a USB device.
- A BIOS password is set.
- The port 443 redirect is removed, and the system can only be accessed by the full URL (<https://<IP>:8443/dma7000>, where <IP> is one of the system's management IP addresses or a host name that resolves to one of those IP addresses).
- For all server-to-server connections, the system requires the remote party to present a valid X.509 certificate. Either the Common Name (CN) or Subject Alternate Name (SAN) field of that certificate must contain the address or host name specified for the server in the Polycom DMA system.

Polycom RMX MCUs don't include their management IP address in the SAN field of the CSR (Certificate Signing Request), so their certificates identify them only by the CN. Therefore, in the Polycom DMA system, an RMX MCU's management interface must be identified by the host name or FQDN specified in the CN field, not by IP address.

Similarly, an Active Directory server certificate often specifies only the FQDN. Therefore, in the Polycom DMA system, the Active Directory must be identified by FQDN, not by IP address.

- The Polycom DMA system can't be integrated with Microsoft Exchange Server and doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.
- Integration with a Polycom CMA system is not supported.
- Superclustering is not supported.
- On the **Login Banner** page, **Enable login banner** is selected and can't be disabled.
- On the **Sessions** page, the **Terminate Session** action is not available.

- On the **Tools** menu, **Top** is removed.
- In the **Add User** and **Edit User** dialog boxes, conference and chairperson passwords are obscured.
- After **Maximum security** is enabled, users must change their passwords.
- If the system is integrated with Microsoft Active Directory, only one local user can have the Administrator role, and no local users can have the Provisioner or Auditor role.

If there are multiple local administrators when you enable **Maximum security**, the system prompts you to choose one local user to retain the Administrator role. All other local users, if any, become conferencing users only and can't log into the management interface.

- If the system is not integrated with Active Directory, each local user can have only one assigned role (Administrator, Provisioner, or Auditor).

If some local users have multiple roles when you enable **Maximum security**, they retain only the highest-ranking role (Administrator > Auditor > Provisioner).

- Local user passwords have stricter limits and constraints (each is set to the noted default if below that level when you enable **Maximum security**):
  - Minimum length is 15-30 characters (default is 15).
  - Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).
  - Maximum number of consecutive repeated characters is 1-4 (default is 2).
  - Number of previous passwords that a user may not re-use is 8-16 (default is 10).
  - Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).
  - Password may not contain the user name or its reverse.
  - Maximum password age is 30-180 days (default is 60).
  - Minimum password age is 1-30 days (default is 1).
- Other configuration settings have stricter limits and constraints (each is set to the noted default if below that level when you enable **Maximum security**):
  - Session configuration limits:
    - » Sessions per system is 4-80 (default is 40).
    - » Sessions per user is 1-10 (default is 5).
    - » Session timeout is 5-60 minutes (default is 10).
  - Local account configuration limits:

- » Local user account is locked after 2-10 failed logins (default is 3) due to invalid password within 1-24 hours (default is 1).
- » Locked account remains locked either until unlocked by an administrator (the default) or for a duration of 1-480 minutes.
- Software build information is not displayed anywhere in the interface.
- You can't restore a backup made before **Maximum security** was enabled.
- File uploads may fail when using the Mozilla Firefox browser unless the proper steps have been taken. See below.

### Enabling File Uploads in Maximum Security with Mozilla Firefox

The Mozilla Firefox browser uses its own certificate database instead of the certificate database of the OS. If you use only that browser to access the Polycom DMA system, the certificate(s) needed to securely connect to the system may be only in the Firefox certificate database and not in the Windows certificate store. This causes a problem for file uploads.

File upload via the Polycom DMA system's Flash-based interface bypasses the browser and creates the TLS/SSL connection itself. Because of that, it uses the Windows certificate store, not the Firefox certificate database. If the certificate(s) establishing trust aren't there, the file upload silently fails.

To avoid this problem, you must import the needed certificates into Internet Explorer (and thus into the Windows certificate store). And, when accessing the system with Firefox, you must use its fully qualified host name.

First, start Internet Explorer and point it to the Polycom DMA system. If you don't receive a security warning, the needed certificates are already in the Windows certificate store.

If you receive a warning, import the needed certificates. The details for doing so depend on the version of Internet Explorer and on your enterprise's implementation of certificates.

In Internet Explorer 7, elect to continue to the site. Then click **Certificate Error** to the right of the address bar and click **View Certificates** to open the **Certificate** dialog box. From there, you can access the Certificate Import Wizard.

The entire trust chain must be imported (the system's signed certificate, intermediate certificates, if any, and the root CA's certificate). When importing a certificate, let Internet Explorer automatically select a certificate store.

See also:

- [“System Security”](#) on page 27
- [“Security Certificates Overview”](#) on page 27
- [“Certificate Settings”](#) on page 31
- [“Security Settings”](#) on page 41
- [“Login Policy Settings”](#) on page 48
- [“Reset System Passwords”](#) on page 52

## Login Policy Settings

The following pages, under **Admin > Login Policy Settings**, let you configure various aspects of user access to the system:

- [Local Password](#)
- [Session](#)
- [Local User Account](#)
- [Banner](#)

See also:

- [“System Security”](#) on page 27
- [“Certificate Settings”](#) on page 31
- [“Security Settings”](#) on page 41

## Local Password

The **Local Password** page lets you increase system security by specifying age, length, and complexity requirements for the passwords of local administrator, auditor, and provisioner users. These rules don't apply to conferencing users' conference and chairperson passcodes, or to Active Directory users.

The following table describes the fields on the **Local Password** page.

**Table 3-6** *Fields on the Local Password Settings page*

Field	Description
<b>Password Management</b>	
Maximum password age (days)	Specify at what age a password expires (30-180 days).
Minimum password age (days)	Specify how frequently a password can be changed (1-30 days).

**Table 3-6** Fields on the Local Password Settings page (continued)

Field	Description
Minimum length	Specify the number of characters a password must contain (8-30).
Minimum changed characters	Specify the number of characters that must be different from the previous password (1-4).
Reject previous passwords	Specify how many of the user's previous passwords the system remembers and won't permit to be reused (8-30).
<b>Password Complexity</b>	
Allow user name or its reverse form	Turns off the protection against a password containing the user's login name or its reverse.
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain.
Numbers	Specify the number of digit characters (0-9) that a password must contain.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same.

See also:

["System Security"](#) on page 27

["Login Policy Settings"](#) on page 48

## Session

The **Session** page lets you increase system security by limiting the number and length of login sessions.

You can see the current login sessions and terminate sessions by going to **User > Login Sessions**. See ["Login Sessions"](#) on page 289.

The following table describes the fields on the **Session** page.

**Table 3-7** *Fields on the Session Settings page*

Field	Description
Active system sessions	Specify the number of simultaneous login sessions by all users or select <b>Unlimited</b> .  Note: If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that's been idle the longest.
Active sessions per user	Specify the number of simultaneous login sessions per user ID or select <b>Unlimited</b> .
Session timeout (minutes)	Specify the length of time after which the system terminates a session for inactivity or select <b>Unlimited</b> .

See also:

[“System Security”](#) on page 27

[“Login Policy Settings”](#) on page 48

## Local User Account

The **Local User Account** page lets you increase system security by:

- Locking 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.
- Disabling accounts that have been inactive a specified number of days.

The following table describes the fields on the **Local User Account** page.

**Table 3-8** *Fields on the Local User Account page*

Field	Description
<b>Account Lockout</b>	
Enable account lockout	Turns on lockout feature and enables lockout configuration fields below.
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account.

**Table 3-8** Fields on the Local User Account page (continued)

Field	Description
Customize user account lockout duration (minutes)	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.
<b>Account Inactivity</b>	
Customize account inactivity threshold (days)	Turns on disabling of inactive accounts and lets you specify the inactivity threshold that triggers disabling.

See also:

["System Security"](#) on page 27

["Login Policy Settings"](#) on page 48

## Banner

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.

The **Banner** page lets you enable the banner and select or create the message it displays. The message may contain up to 1500 characters. If the system is in **Maximum Security** mode, the login banner is enabled and can't be disabled.

The following table describes the fields on the **Banner** page.

**Table 3-9** Fields on the Banner page

Field	Description
Enable login banner	Enables the display of a login banner.  If this box is unchecked, the <b>Message</b> field is disabled. The existing contents, if any, remain unchanged, but aren't displayed to users.
Message	Select one of the messages from the list, or select <b>Custom</b> and type or paste your own message into the field below.  If you select one of the built-in samples, it's copied into the <b>Message</b> field, and you can then edit the copy. When you do so, the system resets the list to <b>Custom</b> . 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.

See also:

[“System Security”](#) on page 27

[“Login Policy Settings”](#) on page 48

## Reset System Passwords

In an extremely high-security environment, security policies may require that all passwords be changed at certain intervals, including operating system passwords.

The **Reset System Passwords** page is available only if the system is in maximum security mode. It lets you change these operating system passwords (such as the password for grub) to new, randomly-generated values. These are passwords for logins that aren't possible on a secure system. Resetting these operating system passwords has no effect on authorized users of the maintenance interface (Administrators, Auditors, and Provisioners) or conferencing users.

### To reset system passwords

- 1 Make sure there are no calls or conferences on the system.
- 2 Go to **Admin > Local Cluster > Reset System Passwords**.
- 3 Click **Reset Passwords**.

The system warns you that active calls and conferences will be terminated and the system will restart, and asks you to confirm.

- 4 Click **Yes**.

The system informs you that the passwords have been reset and that you're being logged out. Then it restarts. This takes several minutes.

- 5 Wait a few minutes to log back in.

See also:

[“System Security”](#) on page 27

[“Security Settings”](#) on page 41

[“The Consequences of Enabling Maximum Security Mode”](#) on page 45

[“Login Policy Settings”](#) on page 48



---

# Local Cluster Configuration

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system configuration topics:

- [Network Settings](#)
- [Time Settings](#)
- [Licenses](#)
- [Signaling Settings](#)
- [Logging Settings](#)
- [Local Cluster Configuration Procedures](#)

These are cluster-specific settings that are not part of the data store shared across superclustered systems. See [“Introduction to the Polycom DMA System”](#) on page 1.

If you’re performing the initial configuration of your Polycom DMA system, study [“Polycom® DMA™ System Initial Configuration Summary”](#) on page 17 before you continue.

## Network Settings

The following table describes the fields on the **Network Settings** page. These values are normally set in the USB Configuration Utility during system installation and rarely need to be changed. See the *Getting Started Guide*.

### Caution

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

If the system is using a CA-provided identity certificate, changing some network settings (host names or IP addresses) also requires you to update the certificate. (If the system is using a self-signed certificate, an updated one is automatically created.)

You can't change these network settings while the system is part of a supercluster or integrated with a Polycom CMA system. You must first leave the supercluster or terminate the integration. If the cluster is responsible for any territories (as primary or backup), reassign those territories. After the change, rejoin the supercluster or Polycom CMA system. See ["Superclustering"](#) on page 195 or ["Polycom CMA System Integration"](#) on page 157.

**Table 4-1** Fields on the Network Settings page

Field	Description
System IP type	IP addressing supported (IPv4, IPv6, or both). <b>Note:</b> Some system features are not supported or not fully tested in an IPv6 environment, including embedded DNS, site topology, and Juniper Networks SRC integration.
System node configuration	Number of nodes (1 or 2) in this cluster.
System split network setting	Specifies whether management and signaling traffic are combined on one network interface or split onto separate interfaces.
<b>Node 1</b>	Status, host name, and IP address(es) of the primary node. The IP type and network setting determine which of the IP fields in this section are enabled. Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
<b>Node 2</b>	Status, host name and IP address(es) of the secondary node. The fields in this section duplicate those in the Node 1 section and are enabled only in two-server configuration.

**Table 4-1** Fields on the Network Settings page (continued)

Field	Description
<b>Shared Management Network Settings</b>	The settings in this section apply to the entire system (both nodes in two-server configuration), whether management and signaling are combined or separate.
Virtual host name	Virtual host name and IP address(es) for the system's management (or combined) network interface. Host names may contain only letters, numbers, and internal dashes (hyphens), and may not include a domain. The reserved values appserv* and dmamgk-* may not be used for host names.
IPv4	
IPv6	
Subnet mask	Subnetwork mask.
IPv6 prefix length	IPv6 CIDR value.
IPv4 gateway	IPv4 address of gateway server for the subnetwork.
Name	The name of the management network interface (eth0) is not editable, and it can't be disabled. The eth0 interface corresponds with the GB1 jack on the server.
Enable	
Auto-negotiation	Turn on <b>Auto-negotiation</b> or set <b>Speed</b> and <b>Duplex</b> manually.
Speed	
Duplex	
Show Link Details	Click to see details about link settings and information. This information may be useful to Polycom Global Services when troubleshooting a network issue.
<b>Shared Signaling Network Settings</b>	The settings in this section are enabled only if management and signaling traffic are on separate networks. If so, they apply to the entire system (both nodes in two-server configuration). The settings are the same as those in <b>Shared Management Network Settings</b> , except that under Signaling Link, the signaling network interface (eth2) can be disabled. This capability exists for debugging purposes. The eth2 interface corresponds with the GB3 jack on the server. (The eth1 interface, which corresponds with the GB2 jack, is reserved for the private network connection between the two nodes in a two-server cluster.)

**Table 4-1** Fields on the Network Settings page (continued)

Field	Description
<b>General System Network Settings</b>	The settings in this section apply to the entire system and aren't specific to management or signaling.
DNS search domains	One or more fully qualified domain names, separated by commas or spaces. The system domain you enter below is added automatically, so you need not enter it.
DNS 1	IP addresses of up to three domain name servers. We strongly recommend specifying at least one DNS server. A DNS server must be specified in order to connect to the Active Directory. See <a href="#">"Microsoft Active Directory Integration"</a> on page 135.
DNS 2	
DNS 3	
Domain	Fully qualified domain name for the system.
Signaling DSCP	The Differentiated Services Code Point value (0 - 63) to put in the DS field of IP packet headers. The DSCP value is used to classify packets for quality of service (QoS) purposes.
Default IPv6 gateway	The interface to use for accessing the IPv6 gateway, generally eth0. Optionally, the gateway's address and the interface, specified as: <code>&lt;IPv6_address&gt;%eth0</code>
Default IPv4 gateway	If management and signaling traffic are on separate networks, select which of the two networks' gateway servers is the default.  Your choice depends on your network configuration and routing. Typically, unless all the endpoints, MCUs, and other devices that communicate with the system are on the same subnet, you'd select the signaling network.

See also:

["Local Cluster Configuration"](#) on page 53

["Routing Configuration Dialog Box"](#) on page 57

["Time Settings"](#) on page 58

["Licenses"](#) on page 59

["Signaling Settings"](#) on page 60

["Logging Settings"](#) on page 63

["Local Cluster Configuration Procedures"](#) on page 64

## Routing Configuration Dialog Box

In the **Network Settings** page's action list, the **Routing Configuration** command opens the **Routing Configuration** dialog box, where you can add or delete network routing rules and view the operating system's underlying routing configuration.

In a split network configuration, routing rules are necessary for proper routing of network traffic. In a combined network configuration, the operating system's underlying routing configuration is likely sufficient unless you need a special rule or rules for your particular network. If you aren't sure, consult the appropriate IT staff or network administrator for your organization.

The following table describes the input fields in the **Routing Configuration** dialog box.

**Table 4-2** *Routing Configuration dialog box*

Field/Column	Description
Subnet mask	The destination network mask for this route.
Length	The destination CIDR subnet.
Interface	In split network configuration, select the interface for this route.
Via	IP address of router for this route. Optional, and only needed for non-default routers.

When you add a routing rule, it appears in the table below the input fields. Select a rule and click **Delete selected route** to delete it. Click **Show raw routing configuration** to display the operating system's underlying routing configuration.

See also:

["Network Settings"](#) on page 54

## Time Settings

The following table describes the fields on the **Time Settings** page. These values are normally set in the USB Configuration Utility during system installation and rarely need to be changed. See the *Getting Started Guide*.

### Caution

Changing time settings requires a system restart and terminates all active conferences.

You can't change the system's time settings while it's integrated with a Polycom CMA system or a supercluster. The integration must first be terminated. See ["Polycom CMA System Integration"](#) on page 157 or ["Superclustering"](#) on page 195. We strongly recommend specifying NTP servers.

**Table 4-3** Fields on the Time Settings page

Field	Description
System time zone	Time zone in which the system is located. We strongly recommend selecting the time zone of a specific geographic location (such as America/Denver), not one of the generic GMT offsets (such as GMT+7). If you really want to use a generic GMT offset, 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.
Auto adjust for Daylight Saving Time	Leave this selected to avoid various potential issues. There is no need to turn this off for geographic time zones that don't implement Daylight Saving Time. The DST adjustment is made only when and where it's appropriate. If you turn this off, the system converts the specific geographic time zone selected into the corresponding generic GMT offset.
Manually set system time	We don't recommend setting time and date manually.
NTP Servers	Specify up to three time servers for maintaining system time (we recommend three). Enter IP addresses or fully qualified domain names.

See also:

[“Local Cluster Configuration”](#) on page 53

[“Network Settings”](#) on page 54

[“Licenses”](#) on page 59

[“Signaling Settings”](#) on page 60

[“Logging Settings”](#) on page 63

[“Local Cluster Configuration Procedures”](#) on page 64

## Licenses

The Polycom DMA system is licensed for the number of concurrent calls it can handle.

The following table describes the fields on the **Licenses** page.

**Table 4-4** *Fields on the Licenses page*

Field	Description
<b>Active License</b>	
Licensed calls	The maximum number of calls that the license enables.
<b>Activation Keys</b>	
A two-server cluster has two sets of the fields below, one for each node in the cluster.	
System serial number	The serial number of the specified server.
Activation key	The activation key you received from Polycom for this server. The key for each server must be the correct one for that server's serial number.

See also:

[“Local Cluster Configuration”](#) on page 53

[“Network Settings”](#) on page 54

[“Time Settings”](#) on page 58

[“Signaling Settings”](#) on page 60

[“Logging Settings”](#) on page 63

[“Local Cluster Configuration Procedures”](#) on page 64

## Signaling Settings

On the **Signaling Settings** page, you can configure H.323, SIP, and XMPP signaling.

### H.323 and SIP Signaling

If H.323 signaling is enabled, the Polycom DMA system's Call Server operates as a gatekeeper, receiving registration requests and calls from H.323 devices. If SIP signaling is enabled, Call Server operates as a SIP registrar and proxy server, receiving registration requests and calls from SIP devices. If both are enabled, the system automatically serves as a SIP <-> H.323 gateway.

Either H.323 signaling, SIP signaling, or both must be enabled in order for the Polycom DMA system's Conference Manager to receive calls for multipoint conferences (virtual meeting rooms, or VMRs) and distribute them among its pool of MCUs.

### XMPP Signaling

If XMPP signaling is enabled, the Polycom DMA system's Call Server operates as an XMPP server, providing chat and presence services to XMPP clients that log into it.

Logins are accepted from any DMA user, local or Active Directory. Clients log in by sending an XMPP login message to the virtual signaling address (IP or FQDN) and XMPP port number of the DMA system, such as:

```
dma1.polycom.com:5223
```

Logged-in clients have presence and chat capability amongst themselves and with clients logged into any federated XMPP service. Federation is automatic and depends simply on DNS resolution of domains.

See [xmpp.org](http://xmpp.org) for more information.

The following table describes the fields on the **Signaling Settings** page.

**Table 4-5** Fields on the Signaling Settings page

Field	Description
<b>H.323 Settings</b>	
Enable H.323 signaling	Enables the system to receive H.323 calls. <b>Caution:</b> Disabling H.323 terminates any existing H.323 calls. When you click <b>Update</b> , the system prompts you to confirm.
Status	Indicates whether the system's H.323 gatekeeper functions are active.



**Table 4-5** Fields on the Signaling Settings page (continued)

Field	Description
H.225 port	Specifies the port number the system's gatekeeper uses for call signaling.  We recommend using the default port number (1720), but you can use any value from 1024 to 65535 that's not already in use and is different from the RAS port.
RAS port	Specifies the port number the system's gatekeeper uses for the RAS (Registration, Admission and Status) channel.  We recommend using the default port number (1719), but you can use any value from 1024 to 65535 that's not already in use and is different from the H.225 port.
H.245 open firewall ports	Shows the port range used for H.245 so you can configure your firewall accordingly. This is display only.
H.323 multicast	Enables the system to support gatekeeper discovery (GRQ messages from endpoints) as described in the H.323 and H.225.0 specifications.
<b>SIP Settings</b>	
Enable SIP signaling	Enables the system to receive Session Initiation Protocol (SIP) calls.  <b>Caution:</b> Disabling SIP terminates any existing SIP calls. When you click <b>Update</b> , the system prompts you to confirm.
Unencrypted SIP port	If <a href="#">Security Settings</a> settings permit unencrypted SIP connections, you can select either TCP or UDP/TCP from the list.  We recommend using the default port number (5060), but you can use any value from 1024 to 65535 that's not already in use and is different from the TLS port.
TLS port	Specifies the port number the system uses for TLS.  We recommend using the default port number (5061), but you can use any value from 1024 to 65535 that's not already in use and is different from the UDP/TCP port.  If SIP signaling is enabled, TLS is automatically supported. Unless unencrypted SIP connections are specifically permitted, TLS must be used. See " <a href="#">Security Settings</a> " on page 41.

**Table 4-5** Fields on the Signaling Settings page (continued)

Field	Description
<b>XMPP Settings</b>	
Enable XMPP signaling	Enables the system to act as an Extensible Messaging and Presence Protocol (XMPP) server for chat and presence services.  Note: Disabling XMPP terminates any existing XMPP calls. When you click <b>Update</b> , the system prompts you to confirm.
Unencrypted XMPP port	If <a href="#">Security Settings</a> page settings permit unencrypted XMPP connections, you can turn it on here.  We recommend using the default port number (5222), but you can use any value from 1024 to 65535 that's not already in use and is different from the TLS port.
TLS port	Specifies the port number the system uses for TLS.  We recommend using the default port number (5223), but you can use any value from 1024 to 65535 that's not already in use and is different from the UDP/TCP port.  If XMPP signaling is enabled, TLS is automatically supported. Unless unencrypted XMPP connections are specifically permitted, TLS must be used. See <a href="#">"Security Settings"</a> on page 41.

See also:

["Local Cluster Configuration"](#) on page 53

["Network Settings"](#) on page 54

["Time Settings"](#) on page 58

["Licenses"](#) on page 59

["Logging Settings"](#) on page 63

["Local Cluster Configuration Procedures"](#) on page 64

## Logging Settings

The following table describes the fields on the **Logging Settings** page.

**Table 4-6** Fields on the Logging Settings page

Field	Description
Logging level	Leave the default, <b>Production</b> , unless advised to change it by Polycom support. <b>Debug</b> is useful for troubleshooting. <b>Verbose debug</b> is not recommended for production systems.
Rolling frequency	If rolling the logs daily (the default) produces logs that are too large, shorten the interval.
Retention period	The number of days to keep log archives. Consider the impact on disk space before lengthening this.
Alert when logs exceed	The percentage of the 1 GB log file capacity in use at which the system displays a warning on the dashboard.
Local log forwarding	<p>Enables you to forward selected log entries to a central log management server (such as <a href="#">Graylog2</a>).</p> <p>Specify:</p> <ul style="list-style-type: none"> <li>The address of the destination server. It must be running some version of syslog.</li> <li>The socket type (transport) for which the destination server's version of syslog is configured. Most versions of syslog support only UDP, the default, but syslog-ng also supports TCP.</li> <li>The facility value. Default is <b>Local0</b>.</li> <li>The log or logs to forward.</li> </ul> <p><b>Note:</b> The DMA system's server.log entries are mapped to syslog-compliant severities (a WARN message from server.log arrives at the destination server. with syslog-compliant WARN level). All other logs being forwarded assigned the syslog-compliant "notice" severity.</p> <p>Each log message is forwarded with its server-side timestamp intact. The receiving syslog adds its own timestamp, but preserving the DMA-applied timestamp makes it easier to accurately troubleshoot time-sensitive events.</p>

See also:

[“Local Cluster Configuration”](#) on page 53

[“Network Settings”](#) on page 54

[“Time Settings”](#) on page 58

[“Licenses”](#) on page 59

[“Signaling Settings”](#) on page 60

[“Local Cluster Configuration Procedures”](#) on page 64

## Local Cluster Configuration Procedures

This section describes the following Polycom DMA 7000 system configuration procedures:

- [Add Licenses](#)
- [Configure Signaling](#)
- [Configure Logging](#)

If you’re performing the initial configuration of your Polycom DMA system, study [“Polycom® DMA™ System Initial Configuration Summary”](#) on page 17 before you continue. Other tasks are required that are described elsewhere.

### Add Licenses

Adding licenses to your Polycom DMA system is a two-step process:

- Request a software activation key code for each server.
- Enter the activation key codes into the system.

The procedures below describe the process.

#### To request a software activation key code for each server

- 1 Log into the Polycom DMA system as an administrator and go to **Admin > Local Cluster > Licenses**.
- 2 Record the serial number for each Polycom DMA server:  
Server A: \_\_\_\_\_  
Server B: \_\_\_\_\_ (none for single-server system)
- 3 Go to <http://www.polycom.com/activation>.
- 4 If you don’t already have one, register for an account. Then log in.
- 5 Select **Product Activation**.

- 6 In the **License Number** field, enter the software license number listed on the first (or only) server's License Certificate (shipped with the product).
- 7 In the **Serial Number** field, enter the first (or only) server's serial number (which you recorded in step 2).
- 8 Click **Generate**.
- 9 When the activation key for the first (or only) server appears, record it:  
Server A: \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_
- 10 If you have a single-server Polycom DMA system, you're finished with this procedure. Continue to the next procedure.
- 11 If you have a two-server cluster, repeat steps 6–8, this time entering the second license number you received and the second server's serial number (also recorded in step 2).

#### Caution

An activation key is linked to a specific server's serial number. For a two-server cluster, you must generate the activation key for each server using that server's serial number. Licensing will fail if you generate both activation keys from the same server serial number.

- 12 When the activation key for the second server appears, record it:  
Server B: \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_

#### To enter license activation key codes

- 1 Go to **Admin > Local Cluster > Licenses**.
- 2 In the **Activation key** field for the first (or only) server, enter the activation key code that was generated for that server's serial number.

#### Caution

An activation key is linked to a specific server's serial number. Each **Activation Key** field is labeled with a serial number. For a two-server cluster, make sure that the activation key code you enter for each server is the correct one for that server's serial number.

- 3 If you have a two-server cluster, in the **Activation key** field for the second server, enter the activation key code that was generated for that server's serial number.
- 4 Click **Update**.  
A dialog box informs you that the licenses have been updated.
- 5 Click **OK**.

See also:

[“Licenses”](#) on page 59

## Configure Signaling

### To configure signaling

- 1 Go to **Admin > Local Cluster > Signaling Settings**.
- 2 To make the system accessible via H.323 calls:
  - a Select **Enable H.323 signaling**.
  - b Leave the default port numbers (1720 for H.225, 1719 for RAS) unless you have a good reason for changing them.
  - c Select **H.323 multicast** to support gatekeeper discovery messages from endpoints.
- 3 To make the system accessible via SIP calls:
  - a Select **Enable SIP signaling**.
  - b If the system’s security settings permit unencrypted SIP connections, optionally select TCP or UDP/TCP from the list.  
  
You must have the Administrator role to change security settings. See [“Security Settings”](#) on page 41.
  - c Leave the default port numbers (5060 for TCP/UDP, 5061 for TLS) unless you have a good reason for changing them.

#### Note

The system only answers UDP calls if that transport is enabled. But for communications back to the endpoint (assuming unencrypted connections are permitted), it uses the transport protocol that the endpoint requested.

For more information about this and other aspects of SIP, see [RFC 3261](#).

- 4 To enable the system’s XMPP server:
  - a Select **Enable XMPP signaling**.
  - b If the system’s security settings permit unencrypted XMPP connections, turn on **Unencrypted XMPP port**.  
  
You must have the Administrator role to change security settings. See [“Security Settings”](#) on page 41.
  - c Leave the default port numbers (5222 for unencrypted XMPP, 5223 for TLS) unless you have a good reason for changing them.
- 5 Click **Update**.  
  
A dialog box informs you that the configuration has been updated.

**6** Click **OK**.

The system processes the configuration. The **Status** field shows the current H.323 signaling state.

See also:

[“Signaling Settings”](#) on page 60

## Configure Logging

**To configure logging**

- 1** Go to **Admin > Local Cluster > Logging Settings**.
- 2** Change **Rolling frequency** and **Retention period** as desired.
- 3** If requested to do so by Polycom support, change **Logging level**.
- 4** Click **Update**.

A dialog box informs you that the configuration has been updated.

**5** Click **OK**.

See also:

[“Logging Settings”](#) on page 63





---

# Device Management

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system's network device management pages:

- [Active Calls](#)
- [Endpoints](#)
- [Site Statistics](#)
- [Site Link Statistics](#)
- [External Gatekeeper](#)
- [External SIP Peer](#)
- [External SBC](#)

Other **Network** menu topics are addressed in the following chapters:

- [“Superclustering”](#) on page 195 (DMAs)
- [“MCU Management”](#) on page 111
- [“Site Topology”](#) on page 241

## Active Calls

The **Active Calls** page lets you monitor the calls in progress (managed by the Call Server) and disconnect an active call.

The search pane above the two lists lets you find calls matching the criteria you specify. Click the down arrow to expand the search pane. You can search for an originator or destination device by its name, alias, or IP address.

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 **Originator** field, it displays calls from 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.

Leave a field empty (or select the blank entry from a list) to match all values.

**Note**

Specifying a filter that includes too many active calls can be a drain on system resources.

The calls that match your search criteria (up to 500) appear in the lower list. You can pin a call that you want to study. This moves it to the upper 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** tabs of the pane on the right. This information (and more) is also available in the **Call Details** dialog box, which appears when you click **Show Call Details** (in the **Actions** list). See [“Call Details Dialog Box”](#) on page 71 for descriptions of the data.

The following table describes the parts of the **Active Calls** list.

**Table 5-1** Information in the Active Calls list

Column	Description
Pin State	Click to pin a call, moving it to the top list and keeping its information available even if the call ends. Click again to unpin it.
Start Time	Time the call began (first signaling event).
Originator	Source of the call (the device's display name, if available; otherwise, its name, alias, or IP address, in that order of preference).
Dial String	Dial string sent by originator.
Destination	Destination of the call (the device's display name, if available; otherwise, its name, alias, or IP address, in that order of preference).
Bit Rate	Bit rate (kbps) of the call. A down arrow indicates that the call was downspeeded. Hover over it to see details.
Class of Service	Class of service (Gold, Silver, or Bronze) of the call.

See also:

[“Device Management”](#) on page 69

[“Call Details Dialog Box”](#) on page 71

[“Endpoints”](#) on page 73

## Call Details Dialog Box

The **Call Details** dialog box appears when you click **Show Call Details** on the **Active Calls** page or **Call History** page. It provides detailed information about the selected call.

The following table describes the fields in the dialog box.

**Table 5-2** Call Details dialog box

Tab/Field/Column	Description
<b>Call Info</b>	
Call Info	Displays the call's: <ul style="list-style-type: none"> <li>• Status (active/ended and pinned/unpinned)</li> <li>• Start time and end time</li> <li>• Duration</li> <li>• Signaling protocol(s)</li> <li>• Polycom DMA server(s) involved</li> <li>• Unique call ID</li> <li>• Dial string</li> </ul>
Originator	Displays the source device's: <ul style="list-style-type: none"> <li>• Name and authentication name</li> <li>• Authentication status</li> <li>• Model and version</li> <li>• Aliases</li> <li>• IP address</li> <li>• Registration status</li> <li>• Site and territory</li> </ul> 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: <ul style="list-style-type: none"> <li>• Name and authentication name</li> <li>• Authentication status</li> <li>• Model and version</li> <li>• Aliases</li> <li>• IP address</li> <li>• Registration status</li> <li>• Site and territory</li> </ul> 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.

**Table 5-2** Call Details dialog box (continued)

Tab/Field/Column	Description
<b>Bandwidth</b>	<p>The table at the top lists each throttlepoint that the call traverses and shows its:</p> <ul style="list-style-type: none"> <li>• Bit rate limit per call (kbps)</li> <li>• Total capacity (kbps)</li> <li>• Used bit rate (kbps) in each class of service</li> <li>• Weight (%)</li> <li>• Territory</li> </ul> <p>If the throttlepoint is a subnet, site, or site link, a link takes you to the corresponding site topology page with the throttlepoint entity selected.</p> <p>Below the table, the data used in bandwidth processing is displayed (all bit rates are kbps):</p> <ul style="list-style-type: none"> <li>• Formal maximum bit rate — the maximum allowed bit rate considering the per call bit rates of each throttlepoint, but not considering total capacity or current usage</li> <li>• Available bit rate capacity in each class of service and for the call's class</li> <li>• Class of service for the call</li> <li>• Minimum downspeed bit rate</li> <li>• Available bit rate limit (%) — the maximum percentage of remaining bandwidth at a throttle point that will be given to any one call (configurable on the <a href="#">Call Server Settings</a> page)</li> <li>• Requested bit rate</li> <li>• Final bit rate</li> </ul>
<b>Call Events</b>	<p>Lists each event in the call and its attributes.</p> <p>When the system is operating as a SIP proxy server, the list includes all SIP signaling messages except 100 TRYING.</p> <p>Hover over an attribute label to see a description. Click <b>Show Message</b> to see the signaling message. Click <b>Show QoS Data</b> to see detailed quality of service statistics.</p>
<b>Property Changes</b>	<p>Lists each property change in the call, showing the value, time, and sequence number of the associated event.</p>
<b>QoS</b>	<p>Quality of service data is only available for H.323 calls. 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.</p> <p>Hover over a data point to see the value at that point.</p>

See also:

[“Active Calls”](#) on page 69

## Endpoints

The **Endpoints** page provides access to information about the devices known to the Polycom DMA system. From it, you can:

- View details about a device.
- View the call history or registration history of a device.
- Add aliases for a device, edit or delete added aliases (but not aliases with which the device registered), and configure the class of service settings.
- Block a device, which prevents it from registering.
- Unblock a blocked device, allowing it to register.
- Quarantine a device, which allows it to register (or remain registered), but not to make or receive calls.
- Remove a quarantined device from quarantine, allowing it to make and receive calls.
- Delete an inactive device or devices. An inactive device is one whose registration has expired. Depending on your **Registration Policy** settings (see [“Registration Policy”](#) on page 227), inactive devices may be automatically deleted after a specified number of days.
- Select multiple devices to block/unblock, quarantine/unquarantine, or delete.
- Manually add a device. The registration status of the device depends on the system’s registration policy (see [“Add Device Dialog Box”](#) on page 78).
- Associate a user with a device.

### Note

If the Polycom DMA system is integrated with a Polycom CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom CMA system.

The search pane above the list lets you find devices matching the criteria you specify. The default search finds all endpoints with active registrations. Click the down arrow to expand the search pane.

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.

Leave a field empty (or select the blank entry from a list) to match all values.

Check **Exceptions** to find devices for which the registration policy script returned an exception. Leave the field to the right empty to match all exception values, or enter a search string to find only exceptions matching that string.

Check **Exceptions** and enter an exclamation point (!) in the field to the right to find only devices with no exceptions.

The devices that match your search criteria (up to 500) are listed below.

The following table describes the parts of the **Endpoints** list.

**Table 5-3** Information in the Endpoints list

Column	Description
Name	The name of the device.
Model	The model designation of the device.
IP Address	The IP address of the device.
Alias	The aliases, if any, assigned to the device.
Site	The site to which the device belongs.
Owner Domain	The domain to which the device's owner, if any, belongs.
Owner	The user who owns the device.
Class of Service	The class of service assigned to the device: <ul style="list-style-type: none"> <li>• Gold</li> <li>• Silver</li> <li>• Bronze</li> <li>• Inherit from associated user (if none, default to Bronze)</li> </ul>
Admission Policy	Indicates the admission policy applied to the device: <ul style="list-style-type: none"> <li>• Allow</li> <li>• Block</li> <li>• Quarantine</li> <li>• Reject</li> </ul>
Compliance Level	Indicates whether the device is compliant or noncompliant with the applicable registration policy script (see " <a href="#">Registration Policy</a> " on page 227).

**Table 5-3** Information in the Endpoints list (continued)

Column	Description
Status	<p>The registration status of the device:</p> <ul style="list-style-type: none"> <li>• <b>Active</b> — The device is registered and can make and receive calls.</li> <li>• <b>Inactive</b> — The device's registration has expired. Whether it can make and receive calls depends on the system's rogue call policy (see "<a href="#">Call Server Settings</a>" on page 205). It can register again.</li> <li>• <b>Quarantined</b> — The device is registered, but it can't make or receive calls. It remains in Quarantined or Quarantined (Inactive) status until you remove it from quarantine.</li> <li>• <b>Quarantined (Inactive)</b> — The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status.</li> <li>• <b>Blocked</b> — The device is not permitted to register. Whether it can make and receive calls depends on the system's rogue call policy. It remains blocked from registering until you unblock it.</li> </ul> <p>A device's status can be determined by:</p> <ul style="list-style-type: none"> <li>• An action by the device.</li> <li>• An action applied to it manually on this page.</li> <li>• The expiration of a timer.</li> <li>• The application of a registration policy and admission policy (see "<a href="#">Registration Policy</a>" on page 227).</li> </ul>
Exceptions	Shows any exceptions with which the device was flagged as a result of applying a registration policy.
Active Calls	Indicates if the device is in a call.

The **Actions** list associated with the **Endpoints** list contains the items in the following table.

**Table 5-4** Endpoint commands

Command	Description
View Details	Opens the <b>Device Details</b> dialog box for the selected endpoint.
Add	Opens the <b>Add Device</b> dialog box, where you can manually add a device to the system.
Edit	Opens the <b>Edit Device</b> dialog box for the selected endpoint, where you can change its information and settings.

**Table 5-4** Endpoint commands

Command	Description
Delete	Removes the registration of the selected endpoint(s) with the Call Server and deletes the endpoint(s) from the Polycom DMA system. A dialog box asks you to confirm.  Unregistered endpoints are treated like rogue endpoints. See <a href="#">“Call Server Settings”</a> on page 205. The device can register again.
Block	Prevents the endpoint(s) from registering with the Call Server. A dialog box asks you to confirm. When blocked endpoints are selected, this becomes <b>Unblock</b> .  Blocked endpoints are treated like rogue endpoints. See <a href="#">“Call Server Settings”</a> on page 205.
Quarantine	Prevents the endpoint(s) from making or receiving calls. A dialog box asks you to confirm. When quarantined endpoints are selected, this becomes <b>Unquarantine</b> .  Unlike a blocked endpoint, a quarantined endpoint is registered (or can register) with the Call Server.
Associate User	Opens the <b>Associate User</b> dialog box for the selected endpoint, where you can associate this device with a user.  Not available if the Polycom DMA system is integrated with a Polycom CMA system. In that case, it receives user-to-device association information from that system.
View Call History	Takes you to <b>Reports &gt; Call History</b> and displays the call history for the selected endpoint.
View Registration History	Takes you to <b>Reports &gt; Registration History</b> and displays the registration history for the selected endpoint.

### Names/Aliases in a Mixed H.323 and SIP Environment

An endpoint that supports both H.323 and SIP can register with the Polycom DMA system’s gatekeeper and SIP registrar using the same name/alias. When the Polycom DMA system receives a call for that endpoint, it uses the protocol of the calling endpoint. This is logical and convenient, but it can lead to failed calls under the following circumstances:

- The system is configured to allow calls to/from rogue (not actively registered) endpoints (see [“Call Server Settings”](#) on page 205).
- 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 Polycom DMA system doesn’t know that the endpoint no longer supports that protocol. When another endpoint tries to call using the called endpoints’ 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.
- Don't allow calls to/from rogue endpoints.
- If you know an endpoint has stopped supporting a protocol, manually delete its inactive registration for that protocol.

### Naming ITP Systems Properly for Bandwidth Management Purposes

An Immersive Telepresence (ITP) room system contains multiple endpoints (codecs). In order for the Polycom DMA system's gatekeeper to recognize these as ITP devices, they must register with names that properly identify them and specify the total number (2, 3, or 4) in the ITP room. For example, the three HDX devices in an OTX 300 ITP system named Bainbridge could register with the following H.323 names:

Bainbridge ITP(1,3)  
Bainbridge ITP(2,3)  
Bainbridge ITP(3,3)

The Polycom DMA system would recognize these three registrations as constituting a single ITP system, assign them a Gold class of service (you can change this if you wish), and treat the three calls from this ITP room as a single call for bandwidth management purposes.

The Polycom DMA system also manages the device registration settings as applying to a single system. You can only edit the device settings for the primary codec (the device designated as 1); the DMA system automatically propagates any changes to the other devices in the ITP system.

This capability is only available for H.323.

Follow this naming convention for the **H.323 Name** field on the **IP Network** page of the HDX web UI. For more information, see the following documents:

- *Administrator's Guide for Polycom HDX Systems*
- *Polycom Immersive Telepresence (ITP) Deployment Guide*
- *Polycom Immersive Telepresence (ITP) Administrator's Guide*

See also:

["Device Management"](#) on page 69

["Add Device Dialog Box"](#) on page 78

["Edit Device Dialog Box"](#) on page 78

["Associate User Dialog Box"](#) on page 80

["Active Calls"](#) on page 69

## Add Device Dialog Box

The **Add Device** dialog box lets you manually add a device to the system.

When you add a device manually, the system applies its registration policy script (see [“Registration Policy”](#) on page 227) to determine the device’s compliance level (compliant or noncompliant with the policy), and then applies the admission policy associated with that result to determine the registration status of the device.

The following table describes the parts of the dialog box.

**Table 5-5** Add Device dialog box

Field	Description
Device type	The device’s signaling protocol (H.323 or SIP).
Signaling address	The H.225 call signaling address (and optionally, port) of the device. Either this or the RAS address is required.
RAS address	The RAS (Registration, Admission and Status) channel address (and optionally, port) of the device.
Aliases	Lists the device’s aliases. When you’re adding a device, this list is empty. The <b>Add</b> button lets you add an alias.
Class of service	Select to specify 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.
Maximum bit rate (kbps)	The maximum bit rate for calls to and from this device.
Minimum downspeed bit rate (kbps)	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.
Model	Optional model number/name for the device.
Version	Optional version information for the device.

See also:

[“Endpoints”](#) on page 73

[“Add Alias Dialog Box”](#) on page 80

[“Edit Alias Dialog Box”](#) on page 80

## Edit Device Dialog Box

The **Edit Device** dialog box lets you change a device’s class of service settings, add aliases, and edit or delete added aliases. You can’t edit or delete aliases with which the device registered.

The following table describes the parts of the dialog box.

**Table 5-6** *Edit Device dialog box*

Field	Description
Name	The name with which the device registered.
Model	The model number/name of the device.
Aliases	Lists the aliases with which the device registered and any aliases that have been added. The <b>Add</b> button lets you add an alias. The <b>Edit</b> and <b>Delete</b> buttons are only available when an added alias is selected.
Site	The site to which the device belongs.
Owner domain	The domain to which the device's owner, if any, belongs.
Owner	The user who owns the device.
Registration status	The registration status of the device.
Permanent	Select to prevent the registration from ever expiring. For MCUs, this option should always be selected.
Class of service	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.
Maximum bit rate (kbps)	The maximum bit rate for calls to and from this device.
Minimum downspeed bit rate (kbps)	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.
Forward if no answer	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.
Forward if busy	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.
Forward unconditionally	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.

See also:

[“Endpoints”](#) on page 73

[“Add Alias Dialog Box”](#) on page 80

[“Edit Alias Dialog Box”](#) on page 80

## Add Alias Dialog Box

The **Add Alias** dialog box lets you specify an alias for the device you’re adding or editing. Enter the alias in the **Value** box and click **OK**.

See also:

[“Endpoints”](#) on page 73

[“Edit Device Dialog Box”](#) on page 78

## Edit Alias Dialog Box

The **Edit Alias** dialog box lets you change the selected alias for the device you’re editing. You can’t edit aliases with which the device registered, only those that have been added. Edit the alias in the **Value** box and click **OK**.

See also:

[“Endpoints”](#) on page 73

[“Edit Device Dialog Box”](#) on page 78

## Associate User Dialog Box

### Note

If the Polycom DMA system is integrated with a Polycom CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom CMA system.

The **Associate User** dialog box lets you associate the selected device with a user. Use the search fields at the top to find the user you want to associate with this device.

You can search by user ID, first name, or last name. The **Search users** field searches all three for matches. The system matches the string you enter against the beginning of the field you’re searching. For instance, if you enter “sa” in the **Last name** field, it displays users whose last names begin with “sa.” To search for a string not at the beginning of the field, you can use an asterisk (\*) as a wildcard.

When you find the right user, select that row and click **OK**. A prompt asks you to confirm associating the endpoint with this user.

See also:

[“Endpoints”](#) on page 73

## Site Statistics

The **Site Statistics** page lists the sites defined in the Polycom DMA system’s site topology and, for those controlled by the system, traffic and QoS statistics. Network clouds and the default internet site aren’t included.

The following table describes the fields in the list.

**Table 5-7** Information in the Site Statistics list

Column	Description
Site Name	Name of the site.
Number of Calls	Number of active calls.
Bandwidth Used %	Percentage of available bandwidth in use.
Bandwidth (Mbps)	Total available bandwidth.
Avg Bit Rate (kbps)	Average bit rate of the active calls. <b>Note:</b> Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate.
Packet Loss %	Average packet loss percentage of the active calls.
Avg Jitter (msec)	Average jitter rate of the active calls.
Avg Delay (msec)	Average delay rate of the active calls.
Territory	Territory to which the site belongs.
Cluster	Cluster responsible for the territory to which the site belongs.

See also:

[“Device Management”](#) on page 69

[“Sites”](#) on page 243

## Site Link Statistics

The **Site Link Statistics** page lists the site links defined in the Polycom DMA system's site topology and, for those controlled by the system, traffic and QoS statistics.

The following table describes the fields in the list.

**Table 5-8** Information in the Site Link Statistics list

Column	Description
Site Link Name	Name of the site link.
Number of Calls	Number of active calls.
Bandwidth Used %	Percentage of available bandwidth in use.
Bandwidth (Mbps)	Total available bandwidth.
Avg Bit Rate (kbps)	Average bit rate of the active calls. <b>Note:</b> Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate.
Packet Loss %	Average packet loss percentage of the active calls.
Avg Jitter (msec)	Average jitter rate of the active calls.
Avg Delay (msec)	Average delay rate of the active calls.
Territory	Territory to which the site belongs.
Cluster	Cluster responsible for the territory to which the site belongs.

See also:

["Device Management"](#) on page 69

["Site Links"](#) on page 254

## External Gatekeeper

On the **External Gatekeeper** page, you can add or remove neighbor gatekeepers. This is a supercluster-wide configuration.

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 appropriate neighbor gatekeeper(s) for resolution.

But note that a Polycom 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 Polycom DMA supercluster may eliminate the need for multiple zones and neighbor gatekeepers.

#### Note

When adding a neighbor gatekeeper, you can only specify one IP address. In an IPv4 + IPv6 environment, to add a neighbor gatekeeper that has both an IPv4 and an IPv6 address, do the following:

- Add the neighbor gatekeeper using its IPv4 address.
- Add it a second time using its IPv6 address.
- Add one **Resolve to external gatekeeper** dial rule (see “[Add Dial Rule Dialog Box](#)” on page 212) that specifies the neighbor gatekeeper’s IPv4 address entry (and no other gatekeepers).
- Add another **Resolve to external gatekeeper** dial rule that specifies the neighbor gatekeeper’s IPv6 address entry (and no other gatekeepers).

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.

The following table describes the fields in the list.

**Table 5-9** *Fields in the External Gatekeeper list*

Column	Description
Name	The name of the neighbored gatekeeper.
Description	Brief description of the gatekeeper.
Address	Host name or IP address of the gatekeeper.
Prefix Range	The dial string prefix(es) assigned to this neighbor gatekeeper. If your dial plan uses the <i>Dial services by prefix</i> 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.
Enabled	Indicates whether the system is using the neighbor gatekeeper.

See also:

“[Device Management](#)” on page 69

“[Add External Gatekeeper Dialog Box](#)” on page 84

“[Edit External Gatekeeper Dialog Box](#)” on page 86

## Add External Gatekeeper Dialog Box

The following table describes the fields in the **Add External Gatekeeper** dialog box.

**Table 5-10** Add External Gatekeeper dialog box

Column	Description
<b>External Gatekeeper</b>	
Enabled	Clearing this check box lets you stop using an external gatekeeper without deleting it.
Name	Gatekeeper name.
Description	The text description displayed in the <b>External Gatekeepers</b> list.
Address	Host name or IP address of the gatekeeper.
RAS port	The RAS (Registration, Admission and Status) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number.
Prefix range	<p>The dial string prefix or prefix range for which the external gatekeeper is responsible.</p> <p>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).</p> <p>If your dial plan uses the <i>Dial services by prefix</i> 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.</p> <p>If your dial plan instead uses a rule that you create to apply the <b>Resolve to external gatekeeper</b> action, there is no need to specify a prefix.</p>
Prefer routed	<p>If selected, the system forces a call to this gatekeeper to routed mode if:</p> <ul style="list-style-type: none"> <li>The gatekeeper is configured with a prefix.</li> <li>The destination signaling address in the gatekeeper's location confirm (LCF) message contains its own IP address (indicating it's in routed mode).</li> </ul> <p>This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.</p>
<b>Authentication Mode</b>	In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.



**Table 5-10** Add External Gatekeeper dialog box

Column	Description
Enabled	Clearing this check box lets you stop sending H.235 credentials to the external gatekeeper without deleting them.
Name	The H.235 name of the Polycom DMA system.
Password Confirm password	The H.235 password for the Polycom DMA system.
Algorithm	Select the encryption algorithm for H.235 authentication.
LRQ test	Click to test the configuration by sending an LRQ message to the external gatekeeper.
<b>Postliminary</b>	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the external gatekeeper.
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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

See also:

[“External Gatekeeper”](#) on page 82

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“Device Authentication”](#) on page 223

## Edit External Gatekeeper Dialog Box

The following table describes the fields in the **Edit External Gatekeeper** dialog box.

**Table 5-11** Edit External Gatekeeper dialog box

Column	Description
<b>External Gatekeeper</b>	
Enabled	Clearing this check box lets you stop using an external gatekeeper without deleting it.
Name	Gatekeeper name.
Description	The text description displayed in the <b>External Gatekeepers</b> list.
Address	Host name or IP address of the gatekeeper.
RAS port	The RAS (Registration, Admission and Status) channel port number. Leave set to 1719 unless you know the gatekeeper is using a non-standard port number.
Prefix range	<p>The dial string prefix or prefix range for which the external gatekeeper is responsible.</p> <p>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).</p> <p>If your dial plan uses the <i>Dial services by prefix</i> 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.</p> <p>If your dial plan instead uses a rule that you create to apply the <b>Resolve to external gatekeeper</b> action, there is no need to specify a prefix.</p>
Prefer routed	<p>If selected, the system forces a call to this gatekeeper to routed mode if:</p> <ul style="list-style-type: none"> <li>The gatekeeper is configured with a prefix.</li> <li>The destination signaling address in the gatekeeper's location confirm (LCF) message contains its own IP address (indicating it's in routed mode).</li> </ul> <p>This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.</p>
<b>Authentication Mode</b>	In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.

**Table 5-11** *Edit External Gatekeeper dialog box*

Column	Description
Enabled	Clearing this check box lets you stop sending H.235 credentials to the external gatekeeper without deleting them.
Name	The H.235 name of the Polycom DMA system.
Password Confirm password	The H.235 password for the Polycom DMA system.
Algorithm	Select the encryption algorithm for H.235 authentication.
LRQ test	Click to test the configuration by sending an LRQ message to the external gatekeeper.
<b>Postliminary</b>	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the external gatekeeper.
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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

See also:

[“External Gatekeeper”](#) on page 82

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“Device Authentication”](#) on page 223

## External SIP Peer

On the **External SIP Peer** page, you can add or remove SIP servers from the list of peer servers to which the system can route calls and from which it may receive calls.

This is a supercluster-wide configuration. But note that a Polycom DMA system supercluster can provide proxy service for any or all domains in the enterprise, allowing the SIP function to be distributed, but managed centrally. This may reduce or eliminate the need for external SIP peer servers.

The following table describes the fields in the list.

**Table 5-12** *Fields in the External SIP Peer list*

Column	Description
Name	The name of the peer server.
Description	Brief description of the peer server.
Peer Address	Fully qualified domain name (FQDN) or IP address of the peer server.
Prefix Range	The dial string prefix(es) assigned to this peer server. If your dial plan uses the <i>Dial services by prefix</i> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this peer server for resolution.
Enabled	Indicates whether the system is using the peer server.
Outbound	Indicates whether the system is registered with the peer so that it can route calls to it.

See also:

[“Device Management”](#) on page 69

[“Add External SIP Peer Dialog Box”](#) on page 89

[“Edit External SIP Peer Dialog Box”](#) on page 94

## Add External SIP Peer Dialog Box

The following table describes the fields in the **Add External SIP Peer** dialog box.

**Table 5-13** Add External SIP Peer dialog box

Field	Description
<b>External SIP Peer</b>	
Enabled	Clearing this check box lets you stop using an external SIP peer server without deleting it.
Name	Peer server name or number. Must be unique among SIP peers.
Description	The text description displayed in the <b>External SIP Peer</b> list.
Next hop address	Fully qualified domain name (FQDN), host name, or IP address of the peer server.  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).
Destination network	Host name or FQDN of the peer server, 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 just the Request-URI for REGISTER messages.  If <b>Type</b> is set to Microsoft, this field is required, is used for the peer's domain, and is implicitly added to the <b>Domain List</b> (if not already there).
Port	The SIP signaling port number. Leave blank to use the default port for each transport protocol (5060 for UDP or TCP transport; 5061 for TLS transport) per RFC 3263. If the peer server is using a non-standard port number, specify it.
Use route header	Add a Route header with the peer's <b>Next hop address</b> 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 <b>Next hop address</b> value for the URI host.

**Table 5-13** Add External SIP Peer dialog box

Field	Description
Prefix range	<p>The dial string prefix(es) assigned to this peer server.</p> <p>Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</p> <p>If your dial plan uses the <i>Dial services by prefix</i> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this peer server for resolution.</p> <p><b>Note:</b> For a SIP peer, the dial string must 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:</p> <p style="padding-left: 40px;">123alice</p> <p>If your dial plan instead uses a rule that you create to apply the <i>Resolve to external SIP peer</i> action, there is no need to specify a prefix.</p>
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.
Type	<p>For a Microsoft Office Communications Server or Lync Server 2010, select <b>Microsoft</b>. Otherwise, select <b>Other</b>.</p> <p>Selecting <b>Microsoft</b> implicitly adds the <b>Destination network</b> value to the <b>Domain List</b> (if not already there) and automatically selects the <b>Postliminary</b> settings that are correct for most deployments with Lync Server 2010, but you can modify them if necessary.</p>
Transport type	The transport protocol to use when contacting this peer server. The default is <b>UDP</b> . <b>Auto detect</b> tells the system to select the protocol as specified in RFC 3263.
Register externally	<p>Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message.</p> <p>Select this option to enable the <b>External Registration</b> tab and configure the system to register with this external peer server, following the rules specified in RFC 3261.</p>
<b>Domain List</b>	<p>If your dial plan uses a rule to apply the <i>Resolve to external SIP peer</i> action, you can restrict calls to this peer server to specific domains by adding the authorized domains to this list.</p> <p>If this list is empty, all domains can resolve to this peer.</p> <p><b>Note:</b> In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict peer servers to specific domains.</p>
Add new domain	Enter a domain and click <b>Add</b> to add it to the list of authorized domains.

**Table 5-13** Add External SIP Peer dialog box

Field	Description
Authorized domains	List of administrative domains, contained in the dial string, for which calls are routed to this peer server. Leave this list empty to route any call that matches the rule to this peer server. Select a domain and click <b>Remove</b> to remove it from the list.
<b>Postliminary</b>	
Use output format	Enables dial string transformations using the To header and Request-URI option settings below instead of a customized script. <b>Note:</b> 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 <b>Use customized script</b> . Making different setting in this section and seeing how the generated script changes can help you learn how to write your own script.
<b>To header options</b>	Specify the format of the To header in messages sent to this peer.
Copy all parameters of original "To" headers	Copies any parameters included in the original To header to the To header sent to this peer. This setting applies to all format options.
Format Template	Select a predefined format from the list, or select <b>Free Form Template</b> and define the format in the associated <b>Template</b> field. The predefined formats in the list and the variables you use in the <b>Template</b> field are described in " <a href="#">SIP Peer Postliminary Output Format Options</a> " on page 99.
<b>Request URI options</b>	Specify the format of the Request-URI.
Format Template	Select a predefined format from the list, or select <b>Free Form Template</b> and define the format in the associated <b>Template</b> field. The predefined formats in the list and the variables you use in the <b>Template</b> field are described in " <a href="#">SIP Peer Postliminary Output Format Options</a> " on page 99.

**Table 5-13** Add External SIP Peer dialog box

Field	Description
Use customized script	<p>Enables an executable script, written in the Javascript language, in the text box below. Writing such a script enables you to more flexibly define dial string and message format transformations to be applied.</p> <p>Type (or paste) the postliminary script you want to apply. Then click <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.</p> <p><b>Note:</b> When you make settings in the <b>Use output format</b> section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script.</p> <p>Making different setting in the <b>Use output format</b> section and seeing how the generated script changes can help you learn how to write your own script.</p>
<b>Authentication</b>	<p>On this tab, you can configure SIP digest authentication, as specified in RFC 3261, for this SIP peer and add or edit authentication credentials.</p> <p>SIP authentication must be enabled and configured on the <a href="#">Device Authentication</a> page.</p>
Authentication	<p>Select one:</p> <ul style="list-style-type: none"> <li>• Handle authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials.</li> <li>• Pass authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server passes it to the source of the request.</li> </ul>



**Table 5-13** Add External SIP Peer dialog box

Field	Description
Proxy authentication	<p>Select one:</p> <ul style="list-style-type: none"> <li>Handle proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials.</li> <li>Pass proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server passes it to the source of the request.</li> </ul>
(table of authentication entries)	<p>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 <b>Add</b> to add authentication credentials.</p> <p>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 <a href="#">Device Authentication</a> page.</p>
<b>External Registration</b>	<p>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.</p>

See also:

[“External SIP Peer”](#) on page 88

[“SIP Peer Postliminary Output Format Options”](#) on page 99

[“Device Authentication”](#) on page 223

[“Add Authentication Dialog Box”](#) on page 103

[“Add Outbound Registration Dialog Box”](#) on page 104

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

## Edit External SIP Peer Dialog Box

The following table describes the fields in the **Edit External SIP Peer** dialog box.

**Table 5-14** Edit External SIP Peer dialog box

Field	Description
<b>External SIP Peer</b>	
Enabled	Clearing this check box lets you stop using an external SIP peer server without deleting it.
Name	Peer server name or number. Must be unique among SIP peers.
Description	The text description displayed in the <b>External SIP Peer</b> list.
Next hop address	Fully qualified domain name (FQDN), host name, or IP address of the peer server.  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).
Destination network	Host name or FQDN of the peer server, 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 just the Request-URI for REGISTER messages.  If <b>Type</b> is set to Microsoft, this field is required, is used for the peer's domain, and is implicitly added to the <b>Domain List</b> (if not already there).
Port	The SIP signaling port number. Leave blank to use the default port for each transport protocol (5060 for UDP or TCP transport; 5061 for TLS transport) per RFC 3263. If the peer server is using a non-standard port number, specify it.
Use route header	Add a Route header with the peer's <b>Next hop address</b> 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 <b>Next hop address</b> value for the URI host.

**Table 5-14** Edit External SIP Peer dialog box

Field	Description
Prefix range	<p>The dial string prefix(es) assigned to this peer server.</p> <p>Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</p> <p>If your dial plan uses the <i>Dial services by prefix</i> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this peer server for resolution.</p> <p><b>Note:</b> For a SIP peer, the dial string must 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:</p> <p style="padding-left: 40px;">123alice</p> <p>If your dial plan instead uses a rule that you create to apply the <i>Resolve to external SIP peer</i> action, there is no need to specify a prefix.</p>
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.
Type	<p>For a Microsoft Office Communications Server or Lync Server 2010, select <b>Microsoft</b>. Otherwise, select <b>Other</b>.</p> <p>Selecting <b>Microsoft</b> implicitly adds the <b>Destination network</b> value to the <b>Domain List</b> (if not already there) and automatically selects the <b>Postliminary</b> settings that are correct for most deployments with Lync Server 2010, but you can modify them if necessary.</p>
Transport type	The transport protocol to use when contacting this peer server. The default is <b>UDP</b> . <b>Auto detect</b> tells the system to select the protocol as specified in RFC 3263.
Register externally	<p>Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message.</p> <p>Select this option to enable the <b>External Registration</b> tab and configure the system to register with this external peer server, following the rules specified in RFC 3261.</p>

**Table 5-14** Edit External SIP Peer dialog box

Field	Description
<b>Domain List</b>	<p>If your dial plan uses a rule to apply the <i>Resolve to external SIP peer</i> action, you can restrict calls to this peer server to specific domains by adding the authorized domains to this list.</p> <p>If this list is empty, all domains can resolve to this peer.</p> <p><b>Note:</b> In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict peer servers to specific domains.</p>
Add new domain	Enter a domain and click <b>Add</b> to add it to the list of authorized domains.
Authorized domains	<p>List of administrative domains, contained in the dial string, for which calls are routed to this peer server.</p> <p>Leave this list empty to route any call that matches the rule to this peer server.</p> <p>Select a domain and click <b>Remove</b> to remove it from the list.</p>
<b>Postliminary</b>	
Use output format	<p>Enables dial string transformations using the To header and Request-URI option settings below instead of a customized script.</p> <p><b>Note:</b> 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 <b>Use customized script</b>.</p> <p>Making different setting in this section and seeing how the generated script changes can help you learn how to write your own script.</p>
<b>To header options</b>	Specify the format of the To header in messages sent to this peer.
Copy all parameters of original "To" headers	Copies any parameters included in the original To header to the To header sent to this peer. This setting applies to all format options.
Format Template	<p>Select a predefined format from the list, or select <b>Free Form Template</b> and define the format in the associated <b>Template</b> field.</p> <p>The predefined formats in the list and the variables you use in the <b>Template</b> field are described in <a href="#">"SIP Peer Postliminary Output Format Options"</a> on page 99.</p>

**Table 5-14** Edit External SIP Peer dialog box

Field	Description
<b>Request URI options</b>	Specify the format of the Request-URI.
Format Template	<p>Select a predefined format from the list, or select <b>Free Form Template</b> and define the format in the associated <b>Template</b> field.</p> <p>The predefined formats in the list and the variables you use in the <b>Template</b> field are described in <a href="#">“SIP Peer Postliminary Output Format Options”</a> on page 99.</p>
Use customized script	<p>Enables an executable script, written in the Javascript language, in the text box below. Writing such a script enables you to more flexibly define dial string and message format transformations to be applied.</p> <p>Type (or paste) the postliminary script you want to apply. Then click <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.</p> <p><b>Note:</b> When you make settings in the <b>Use output format</b> section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script.</p> <p>Making different setting in the <b>Use output format</b> section and seeing how the generated script changes can help you learn how to write your own script.</p>
<b>Authentication</b>	<p>On this tab, you can configure SIP digest authentication, as specified in RFC 3261, for this SIP peer and add or edit authentication credentials.</p> <p>SIP authentication must be enabled and configured on the <a href="#">Device Authentication</a> page.</p>
Authentication	<p>Select one:</p> <ul style="list-style-type: none"> <li>• Handle authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials.</li> <li>• Pass authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server passes it to the source of the request.</li> </ul>

**Table 5-14** Edit External SIP Peer dialog box

Field	Description
Proxy authentication	<p>Select one:</p> <ul style="list-style-type: none"> <li>Handle proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials.</li> <li>Pass proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server passes it to the source of the request.</li> </ul>
(table of authentication entries)	<p>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 <b>Add</b> to add authentication credentials.</p> <p>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 <a href="#">Device Authentication</a> page.</p>
<b>External Registration</b>	<p>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.</p>

See also:

[“External SIP Peer”](#) on page 88

[“SIP Peer Postliminary Output Format Options”](#) on page 99

[“Device Authentication”](#) on page 223

[“Add Authentication Dialog Box”](#) on page 103

[“Edit Authentication Dialog Box”](#) on page 103

[“Add Outbound Registration Dialog Box”](#) on page 104

[“Edit Outbound Registration Dialog Box”](#) on page 105

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

## SIP Peer Postliminary Output Format Options

This section includes the following information to help with the postliminary settings for an external SIP peer:

- [To Header Format Options](#)
- [Request-URI Format Options](#)
- [Free Form Template Variables](#)
- [To Header and Request-URI Examples](#)

### 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. See "[Free Form Template Variables](#)" on page 101 and "[To Header and Request-URI Examples](#)" on page 101.

## Request-URI Format Options

The settings available on the **Format** list for the Request-URI 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#

**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:#phost#:#pport#;transport=#ptransport#

**Free Form Template** – Format defined in associated **Template** field is used without further modification. See [“Free Form Template Variables”](#) on page 101 and [“To Header and Request-URI Examples”](#) on page 101.



## Free Form Template Variables

In the **Template** fields on the **Postliminary** tab, and when specifying a Request-URI or other headers for outbound registration (see [“Add Outbound Registration Dialog Box”](#) on page 104), you can use the variables in the table below 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 5-15** Variables for use in SIP Peer Postliminary Template fields

Variable	Description
otdisplay	Original To header's display name.
otuser	User portion of the original request's To header URL field.
othost	Host/IP portion of the original request's To header URL field.
otscheme	Original To header's URL scheme (sip, sips, tel).
phost	Peer's configured IP/FQDN.
pscheme	Peer's configured scheme based on transport (sip, sips).
oruser	User portion of the original request's Request-URL field.
orhost	Host/IP portion of the original request's Request-URL field.
orscheme	Original request's URL scheme.
pnetORhost	Destination network parameter if specified, otherwise the peer's configured IP/FQDN.

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. For the To header, the contents of the **Template** field specify the complete header except for the header name (“To”).

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

## To Header and Request-URI Examples

The tables below show some examples of To header and Request-URI transformations using the variables described in [“Free Form Template Variables”](#) on page 101.

**Table 5-16** To header examples

Original	Template	Result
sip:user@host	#orscheme#atest	sip:atest
sip:user@host	#orscheme##oruser#@#orhost#	sip:user@host
sip:host	#orscheme##oruser#@foo.bar	sip:host
sip:user@host	#orscheme##oruser#@foo.bar	sip:user@foo.bar
sip:host	sips:#oruser#@foo.bar	sips:foo.bar
sip:user@host	#orscheme##oruser#@#othost#	sip:user@toHeaderUrIHost

**Table 5-17** Request-URI header examples

Original	Template	Result
displayname <sip:user@host>	#otdisplay# <sip:#otuser#@#othost#>	displayname <sip:user@host>
displayname <sip:user@host>	<#otscheme##otuser#@#othost#>	<sip:user@host>
displayname <sip:user@host>	<sip:#otuser#@#othost#>	<sip:user@host>
displayname <sip:user@host>	#otdisplay# <sip:#otuser#@#phost#>	displayname <sip:user@peerHostIp>
displayname <sip:user@host>	#otdisplay# <sip:#otuser#@foo.bar>	displayname <sip:user@foo.bar>

See also:

[“External SIP Peer”](#) on page 88

[“Add External SIP Peer Dialog Box”](#) on page 89

[“Edit External SIP Peer Dialog Box”](#) on page 94

[“Add Outbound Registration Dialog Box”](#) on page 104

[“Edit Outbound Registration Dialog Box”](#) on page 105

## Add Authentication Dialog Box

The **Add Authentication** dialog box lets you add an authentication credential entry either for a specific external SIP peer (see [“Edit External SIP Peer Dialog Box”](#) on page 94) or to the general list of outbound authentication credentials for the system (see [“Device Authentication”](#) on page 226).

The following table describes the fields in the dialog box.

**Table 5-18** Add Authentication dialog box

Field	Description
Realm	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.
User name	The user name to use for authentications in this realm.
Password Confirm password	The password to use for authentications in this realm.

See also:

[“External SIP Peer”](#) on page 88

[“Add External SIP Peer Dialog Box”](#) on page 89

[“Edit External SIP Peer Dialog Box”](#) on page 94

## Edit Authentication Dialog Box

The **Edit Authentication** dialog box lets you edit an authentication credential entry either for a specific external SIP peer (see [“Edit External SIP Peer Dialog Box”](#) on page 94) or from the general list of outbound credentials for the system (see [“Device Authentication”](#) on page 226).

The following table describes the fields in the **Edit Authentication** dialog box.

**Table 5-19** Edit Authentication dialog box

Field	Description
Realm	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.
User name	The user name to use for authentications in this realm.
Password Confirm password	The password to use for authentications in this realm.

See also:

[“External SIP Peer”](#) on page 88

[“Add External SIP Peer Dialog Box”](#) on page 89

[“Edit External SIP Peer Dialog Box”](#) on page 94

## Add Outbound Registration Dialog Box

Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message. The **Add Outbound Registration** dialog box lets you add outbound registration configurations that the system can use to register with the SIP peer that you’re adding or editing, following the rules specified in RFC 3261.

The following table describes the fields in the **Add Outbound Registration** dialog box.

**Table 5-20** Add Outbound Registration dialog box

Field	Description
Enabled	Clearing this check box lets you stop using this registration without deleting the registration information.
Address of record	The AOR with which the system registers (see registration rules in RFC 3261), such as: sip:1000@dma.polycom.com
Territory to perform registration	Responsibility for registering must be assigned to a territory, thus making the primary or backup DMA cluster for the territory responsible, depending on which is active.
Contact address format	Select <b>IP</b> or <b>DNS</b> 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 <b>Free Form</b> to specify that the contact header should use the FQDN you enter. The external peer must be able to resolve this FQDN.
User name	The user name to use for the authentication credentials if the external peer challenges the registration request.

**Table 5-20** Add Outbound Registration dialog box

Field	Description
Password Confirm password	The password to use for the authentication credentials if the external peer challenges the registration request.
Request-URI	The Request-URI to include when registering with this SIP peer, specified using the variables (#delimited) defined in “Free Form Template Variables” on page 101.
Other headers	Additional headers to include when registering with this SIP peer.  Click <b>Add</b> to add a header. In the <b>Add Header</b> dialog box, specify the header name and value(s), using the variables (#delimited) defined in “Free Form Template Variables” on page 101.  Click <b>Edit</b> or <b>Delete</b> to edit or delete the selected header.

See also:

“External SIP Peer” on page 88

“Add External SIP Peer Dialog Box” on page 89

“Edit External SIP Peer Dialog Box” on page 94

## Edit Outbound Registration Dialog Box

Some external SIP peers require peer proxies to register with them as an endpoint does, using a REGISTER message. The **Edit Outbound Registration** dialog box lets you edit the selected outbound registration configuration.

The following table describes the fields in the **Edit Outbound Registration** dialog box.

**Table 5-21** Edit Outbound Registration dialog box

Field	Description
Enabled	Clearing this check box lets you stop using this registration without deleting the registration information.
Address of record	The AOR with which the system registers (see registration rules in RFC 3261), such as:  sip:1000@dma.polycom.com
Territory to perform registration	Responsibility for registering must be assigned to a territory, thus making the primary or backup DMA cluster for the territory responsible, depending on which is active.

**Table 5-21** Edit Outbound Registration dialog box

Field	Description
Contact address format	Select <b>IP</b> or <b>DNS</b> 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 <b>Free Form</b> to specify that the contact header should use the FQDN you enter. The external peer must be able to resolve this FQDN.
User name	The user name to use for the authentication credentials if the external peer challenges the registration request.
Password Confirm password	The password to use for the authentication credentials if the external peer challenges the registration request.
Request-URI	The Request-URI to include when registering with this SIP peer, specified using the variables (#delimited) defined in <a href="#">“Free Form Template Variables”</a> on page 101.
Other headers	Additional headers to include when registering with this SIP peer.  Click <b>Add</b> to add a header. In the <b>Add Header</b> dialog box, specify the header name and value(s), using the variables (#delimited) defined in <a href="#">“Free Form Template Variables”</a> on page 101.  Click <b>Edit</b> or <b>Delete</b> to edit or delete the selected header.

See also:

[“External SIP Peer”](#) on page 88

[“Add External SIP Peer Dialog Box”](#) on page 89

[“Edit External SIP Peer Dialog Box”](#) on page 94

## External SBC

On the **External SBC** page, you can add or remove SBC (session border controller) units (Polycom VBP appliances are supported) from the list of such devices that the system can use. In an H.323 environment, SBCs regulate access across the firewall.

This is a supercluster-wide configuration.

For most configurations, SBCs should be configured on a per site basis on the [Sites](#) page. There are three reasons to configure an SBC on the **External SBC** page:

- To create a prefix service that allows dialing through the specific SBC by prefix.
- To define a postliminary script to be applied when dialing through the SBC.
- For bandwidth management.

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

The following table describes the fields in the list.

**Table 5-22** *Fields in the External SBC list*

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

See also:

[“Device Management”](#) on page 69

[“Add External SBC Dialog Box”](#) on page 108

[“Edit External SBC Dialog Box”](#) on page 109

## Add External SBC Dialog Box

The following table describes the fields in the **Add External SBC** dialog box.

**Table 5-23** Add External SBC dialog box

Column	Description
<b>External SBC</b>	
Name	SBC unit name.
Description	The text description displayed in the <b>External SBC</b> list.
Address	Host name or IP address of the SBC.
Port	The SBC's port number. Leave set to 1720 unless you know the unit is using a non-standard port number.
Prefix range	<p>The dial string prefix or prefix range for which the external SBC is responsible.</p> <p>Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</p> <p>If your dial plan uses the <i>Dial services by prefix</i> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.</p> <p>If you don't specify prefixes, the dial plan can use the <i>Dial external networks by H.323 URL or SIP URI</i> dial rule or the <i>Dial endpoints by IP address</i> dial rule (both are in the default dial plan) to contact addresses outside the enterprise network. The system detects that firewall traversal is needed and routes the call through the SBC closest to the caller. This must be configured per site on the H.323 Routing tab of the <b>Add Site</b> or <b>Edit Site</b> dialog (see "<a href="#">Edit Site Dialog Box</a>" on page 248).</p>
Enabled	Clearing this check box lets you stop using an external SBC without deleting it.
<b>Postliminary</b>	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the external 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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.



See also:

[“External SBC”](#) on page 106

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

## Edit External SBC Dialog Box

The following table describes the fields in the **Edit External SBC** dialog box.

**Table 5-24** *Edit External SBC dialog box*

Column	Description
<b>External SBC</b>	
Name	SBC unit name.
Description	The text description displayed in the <b>External SBC</b> list.
Address	Host name or IP address of the SBC.
Port	The SBC’s port number. Leave set to 1720 unless you know the unit is using a non-standard port number.
Prefix range	<p>The dial string prefix or prefix range for which the external SBC is responsible.</p> <p>Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)</p> <p>If your dial plan uses the <i>Dial services by prefix</i> dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.</p> <p>If you don’t specify prefixes, the dial plan can use the <i>Dial external networks by H.323 URL or SIP URI</i> dial rule or the <i>Dial endpoints by IP address</i> dial rule (both are in the default dial plan) to contact addresses outside the enterprise network. The system detects that firewall traversal is needed and routes the call through the SBC closest to the caller. This must be configured per site on the H.323 Routing tab of the <b>Add Site</b> or <b>Edit Site</b> dialog (see <a href="#">“Edit Site Dialog Box”</a> on page 248).</p>
Enabled	Clearing this check box lets you stop using an external SBC without deleting it.

**Table 5-24** *Edit External SBC dialog box*

Column	Description
Postliminary	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the external 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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

See also:

[“External SBC”](#) on page 106

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

---

# MCU Management

This chapter describes the Polycom® Distributed Media Application™ (DMA™) 7000 system's MCU management tools and tasks:

- [MCUs](#)
- [MCU Pools](#)
- [MCU Pool Orders](#)

## Note

MCU pools were called MCU zones in earlier versions of the Polycom DMA system. The name was changed to avoid confusion with the concept of gatekeeper zones.

The Polycom DMA system uses MCU pools and pool orders to select the MCU on which to host a conference. It's important that you understand how MCU pools and pool orders work, and that you set them up in a way that uses the MCUs in your enterprise effectively as conferencing resources.

## MCUs

The **MCUs** page shows the MCUs, or media servers, known to the Polycom DMA system. In a superclustered system, this list encompasses all MCUs throughout the supercluster and is the same on all clusters in the supercluster. It includes:

- MCUs that are available as a conferencing resource for the Polycom DMA system's Conference Manager function (enabled for conference rooms), but aren't registered with the Call Server. Up to 64 MCUs can be enabled for conference rooms.
- MCUs that are registered with the Polycom 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.

An MCU can appear in this list either because it registered with the Call Server or because it was manually added. If the MCU registered itself, it can be used as a standalone MCU. But to use such an MCU as a conferencing resource, you must edit its entry to enable it for conference rooms and provide the additional configuration information required.

You must organize MCUs configured as conferencing resources into one or more MCU pools (logical groupings of media servers). Then, you can define one or more MCU pool orders that specify the order of preference in which MCU pools are used.

Every conference room (VMR) is associated with an MCU pool order. 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. See [“MCU Pools”](#) on page 127 and [“MCU Pool Orders”](#) on page 130.

#### Note

For H.323 calls to a conference room (virtual meeting room, or VMR), the Polycom DMA system can only do bandwidth management if the MCU hosting the conference room is registered with it (in a supercluster, with any cluster). If the MCU is unregistered, or is registered to another gatekeeper (not part of the supercluster), the bandwidth for the call is not counted for bandwidth management, site statistics, or the network usage report.

In a SIP signaling environment, in order for a Polycom RMX MCU to register with the Polycom 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 not present.

In order for the Polycom DMA system to assign an alternate gatekeeper to an MCU, that MCU must be in a site that belongs to a territory which has a backup Polycom DMA system assigned to it.

#### Note













This version of the Polycom DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as part of the Conference Manager’s conferencing resource pool, but their Media Port Reservation feature is not supported. This feature must be set to Disabled on Cisco Codian MCUs in order to use them as part of the Conference Manager’s conferencing resource pool.

This version of the Polycom DMA system supports the use of Polycom MGC MCUs, but not as part of the Conference Manager’s conferencing resource pool. They can register with the Call Server as standalone MCUs and/or ISDN gateways.

When a Polycom RMX MCU is functioning as an ISDN gateway, each call through the gateway consumes two ports, one for the ISDN side and one for the H.323 side. The ports used for gateway calls aren’t available for conferences, so gateway operations may significantly reduce the available conferencing resources.

The following table describes the fields in the list (the **View Details** command lets you see this information in a more readable form for the selected MCU).

**Table 6-1** Information in the MCU list

Column	Description
	<p>Connection and service status and capabilities:</p> <p> Connected       Disconnected</p> <p> Connected securely (encrypted connection)</p> <p> In service       Out of service</p> <p> Busied out       Not licensed</p> <p> Supports conference recording</p> <p> Doesn't support conference recording</p> <p> Supports shared number dialing IVR service</p> <p> Functions as a gateway</p> <p> Warning</p> <p>Hover over an icon to see the associated status message.</p>
Name	The name of the MCU.
Model	The type of MCU.
Version	The version of software on the MCU.
IP Addresses	The IP address for the MCU's management interface (M) and signaling interface (S).
Signaling Type	The type of signaling for which the MCU is configured: H.323, SIP, or both.
Ports Reserved	<p>The number of video and voice ports on the MCU that are reserved for the Polycom CMA system and therefore off-limits to the Polycom DMA system Applies only to MCUs that are enabled for conference rooms (available as a conferencing resource for the Polycom DMA system's Conference Manager function).</p> <p>Reserving a portion of an MCU's capacity for the Polycom CMA system enables that portion to be used for scheduled conferences (where MCU resources are reserved in advance).</p> <p>This feature is available only on RMX v. 6.0 or later MCUs.</p>

**Table 6-1** Information in the MCU list

Column	Description
Prefix	The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. MCUs don't need a prefix to be used as conferencing resources by the Conference Manager.
Registration Status	<p>The registration status of the device:</p> <ul style="list-style-type: none"> <li>Active — The device is registered and can make and receive calls.</li> <li>Inactive — The device's registration has expired. Whether it can make and receive calls depends on the system's rogue call policy (see <a href="#">"Call Server Settings"</a> on page 205). It can register again.</li> <li>Quarantined — The device is registered, but it can't make or receive calls. It remains in Quarantined or Quarantined (Inactive) status until you remove it from quarantine.</li> <li>Quarantined (Inactive) — The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status.</li> <li>Blocked — The device is not permitted to register. Whether it can make and receive calls depends on the system's rogue call policy. It remains blocked from registering until you unblock it.</li> </ul> <p>A device's status can be determined by:</p> <ul style="list-style-type: none"> <li>An action by the device.</li> <li>An action applied to it manually on this page.</li> <li>The expiration of a timer.</li> <li>The application of a registration policy and admission policy (see <a href="#">"Registration Policy"</a> on page 227).</li> </ul>
Exceptions	Shows any exceptions with which the device was flagged as a result of applying a registration policy.
MCU Pools	The MCU pools in which this MCU is used, if it's enabled for conference rooms (available as a conferencing resource for the Polycom DMA system's Conference Manager function).
Site	The site in which the MCU is located. See <a href="#">"Sites"</a> on page 243.

The **Actions** list associated with the **MCU** list contains the items in the following table.

**Table 6-2** *MCU commands*

Command	Description
View Details	Opens the <b>Device Details</b> dialog box for the selected MCU.
Add	Opens the <b>Add MCU</b> dialog box, where you can add an MCU to the pool of devices known to the Polycom DMA system.
Edit	Opens the <b>Edit MCU</b> dialog box for the selected MCU, where you can change its information and settings.
Delete	Removes the selected MCU from the pool of devices that are available to the Polycom DMA system as conferencing resources. A dialog box asks you to confirm.  Also removes the MCU's registration with the Call Server, disabling prefix dialing until the MCU re-registers.
Start Using	Enables the Polycom DMA system to start using the selected MCU as a conferencing resource or ISDN gateway (for simplified gateway dialing).  This command only affects Conference Manager and simplified gateway dialing functionality. It doesn't affect MCUs that are simply registered with the Call Server.
Stop Using	Stops the Polycom DMA system from using the selected MCU as a conferencing resource or ISDN gateway. A dialog box asks you to confirm. If you do so, existing calls on the MCU are terminated or (for SIP calls only) migrated to in-service MCUs with available capacity.  If the MCU is an ISDN gateway, the system stops using it for simplified gateway dialing.  This command immediately terminates the system's use of the MCU as a conferencing resource or ISDN gateway. It has no effect on the MCU itself, which continues to accept any calls from other sources.
Busy Out	Stops the Polycom DMA system from creating new conferences on the selected MCU, but allows its existing conferences to continue and accepts new calls to those conferences. A dialog box asks you to confirm.  If the MCU is an ISDN gateway, the system stops using it for simplified gateway dialing.  This gracefully winds down the system's use of the MCU as a conferencing resource. It has no effect on the MCU itself, which continues to accept any calls from other sources.

**Table 6-2** MCU commands

Command	Description
Quarantine	Allows the MCU to register (or remain registered), but not to make or receive calls. If the selected MCU is quarantined, this becomes <b>Unquarantine</b> .
Block	Prevents the selected MCU from registering. If the selected MCU is blocked, this becomes <b>Unblock</b> .

**Note**

In the recommended high security mode, the Polycom DMA system uses only HTTPS for the conference control connection to MCUs, and you must configure your MCUs to accept encrypted connections. We recommend doing so. When unencrypted connections are used, the MCU login name and password are sent unencrypted over the network.

The Polycom DMA system knows only what resources an MCU has currently available. It can't know what's been scheduled for future use.

To use the same RMX MCU (RMX v6.0 and above) for both reservationless and scheduled conferences, determine how many ports you want to set aside for scheduled conferences and designate those as **Ports reserved for CMA system** so that the Polycom DMA system won't use them. This feature is not available for Cisco Codian MCUs.

The Automatic Password Generation feature, introduced in RMX version 7.0.2, is not compatible with the Polycom DMA system. On Polycom RMX MCUs to be used with the Polycom 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).

See also:

[“Add MCU Dialog Box”](#) on page 117

[“Edit MCU Dialog Box”](#) on page 120

[“MCU Procedures”](#) on page 124

[“MCU Pools”](#) on page 127

[“MCU Pool Orders”](#) on page 130



## Add MCU Dialog Box

Lets you add an MCU, gateway, or combination of the two to the pool of devices available to the Polycom DMA system.

### Note

This version of the Polycom DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as part of the Conference Manager's conferencing resource pool, but their Media Port Reservation feature is not supported. This feature must be set to Disabled on Cisco Codian MCUs in order to use them as part of the Conference Manager's conferencing resource pool.

This version of the Polycom DMA system supports the use of Polycom MGC MCUs, but not as part of the Conference Manager's conferencing resource pool. They can register with the Call Server as standalone MCUs and/or gateways.

When a Polycom RMX MCU is functioning as an ISDN gateway, each call through the gateway consumes two ports, one for the ISDN side and one for the H.323 side. The ports used for gateway calls aren't available for conferences, so gateway operations may significantly reduce the available conferencing resources.

The following table describes the fields in the dialog box.

**Table 6-3** Add MCU dialog box

Field	Description
<b>External MCU</b>	
Name	Host name of the MCU.
Management IP	IP address for logging into the MCU (to use it as a conferencing resource).
Admin ID	Administrative user ID with which the Polycom DMA system can log into the MCU. For a maximum security environment, this must be a machine account created on the RMX MCU. Note that the RMX MCU uses case-sensitive machine names (and thus FQDNs) when creating machine accounts.
Password	Password for the administrative user ID.
Video ports reserved for CMA system	The number of video ports on this MCU that are off-limits to the Polycom DMA system. Set this to the number of ports you want to reserve for scheduled conferences (requires RMX v6.0 or later).
Voice ports reserved for CMA system	The number of voice ports on this MCU that are off-limits to the Polycom DMA system. Set this to the number of ports you want to reserve for scheduled conferences (requires RMX v6.0 or later).

**Table 6-3** Add MCU dialog box

Field	Description
Type	Lists the types of MCU the system supports. Must be set to the correct MCU type in order for the DMA system to be able to connect to it.
Direct dial in prefix	The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. MCUs don't need a prefix to be used as conferencing resources by the Conference Manager.
Signaling address for H.323	The address that the MCU uses for H.323 signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and H.323 is enabled, this field is required.
Signaling address for SIP	The address that the MCU uses for SIP signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and SIP is enabled, this field is required.
Transport type	The SIP transport type to use with this MCU. If the Polycom DMA system's security settings don't allow unencrypted connections, this must be TLS.
Signaling type	Select SIP, H.323, or both, depending on how the Polycom DMA system and MCU are configured.
Enable for conference rooms	Makes the MCU available as a conferencing resource for the Polycom DMA system's Conference Manager. Up to 64 MCUs can be enabled for conference rooms.
ISDN gateway	Makes the MCU available as an ISDN gateway device and enables the <b>ISDN Gateway</b> tab for configuring the gateway.
Class of service	Select to specify the default class of service and the bit rate limits for this MCU. If specified, calls to the MCU use its class of service or the calling endpoint's, whichever is better.
Maximum bit rate (kbps)	Select the maximum bit rate for calls to this MCU.
Minimum downspeed bit rate (kbps)	Select the minimum bit rate to which calls to this MCU can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped. The minimum that applies to a call is the higher of the MCU's and the calling endpoint's.

**Table 6-3** Add MCU dialog box

Field	Description
<b>ISDN Gateway</b>	
Copy from entry for ISDN gateway	Lets you copy the delimiter and session profiles from another ISDN gateway instead of entering them below. This is especially useful for MGC devices because each ISDN network card must be registered separately, but all cards support the same gateway configuration.
Dial string delimiter	The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number.
Session Profile table	Lists the defined session profile prefixes. A session profile prefix is a numeric dial string prefix that specifies a bit rate for the call and which protocols it supports. Click <b>Add</b> to add a session profile. Click <b>Edit</b> or <b>Delete</b> to change or delete the selected session profile. You can't change or delete session profiles that the gateway registered with, only those that you added.
<b>Media IP Addresses</b>	
Add new media IP address	If you specify the login information for the MCU, the system can get media addresses from the MCU. If not, enter an IP address for media streams and click <b>Add</b> to add it the list below.
Media IP addresses	List of media addresses for the MCU. Click <b>Remove</b> to delete the selected address.
<b>Postliminary</b>	
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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

See also:

["MCUs"](#) on page 111

["MCU Procedures"](#) on page 124

["Add Session Profile Dialog Box"](#) on page 123

["Edit Session Profile Dialog Box"](#) on page 123

["Script Debugging Dialog Box for Preliminaries/Postliminaries"](#) on page 215

## Edit MCU Dialog Box

Lets you edit an MCU. If you intend to edit the login information for the MCU (**Management IP, Admin ID, or Password**), you must first stop using the MCU (terminating existing calls and conferences) or busy it out and wait for existing calls and conferences to end.

### Note

This version of the Polycom DMA system supports the use of Cisco Codian 4200, 4500, and MSE 8000 series MCUs as part of the Conference Manager's conferencing resource pool, but their Media Port Reservation feature is not supported. This feature must be set to Disabled on Cisco Codian MCUs in order to use them as part of the Conference Manager's conferencing resource pool.

This version of the Polycom DMA system supports the use of Polycom MGC MCUs, but not as part of the Conference Manager's conferencing resource pool. They can register with the Call Server as standalone MCUs and/or gateways.

When a Polycom RMX MCU is functioning as an ISDN gateway, each call through the gateway consumes two ports, one for the ISDN side and one for the H.323 side. The ports used for gateway calls aren't available for conferences, so gateway operations may significantly reduce the available conferencing resources.

The following table describes the fields in the dialog box.

**Table 6-4** Edit MCU dialog box

Field	Description
<b>External MCU</b>	
Name	Host name of the MCU.
Management IP	IP address for logging into the MCU (to use it as a conferencing resource).
Admin ID	Administrative user ID with which the Polycom DMA system can log into the MCU. For a maximum security environment, this must be a machine account created on the RMX MCU. Note that the RMX MCU uses case-sensitive machine names (and thus FQDNs) when creating machine accounts.
Password	Password for the administrative user ID.
Video ports reserved for CMA system	The number of video ports on this MCU that are off-limits to the Polycom DMA system. Set this to the number of ports you want to reserve for scheduled conferences (requires RMX v6.0 or later).
Voice ports reserved for CMA system	The number of voice ports on this MCU that are off-limits to the Polycom DMA system. Set this to the number of ports you want to reserve for scheduled conferences (requires RMX v6.0 or later).

**Table 6-4** Edit MCU dialog box

Field	Description
Type	Lists the types of MCU the system supports. Must be set to the correct MCU type in order for the DMA system to be able to connect to it.
Direct dial in prefix	The dialing prefix assigned to the MCU, if any. MCUs without a prefix are unavailable for direct prefix-based dialing. MCUs don't need a prefix to be used as conferencing resources by the Conference Manager.
Signaling address for H.323	The address that the MCU uses for H.323 signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and H.323 is enabled, this field is required.
Signaling address for SIP	The address that the MCU uses for SIP signaling. If you specify the login information for the MCU, this field is optional (the system can get the address from the MCU). If not, and SIP is enabled, this field is required.
Transport type	The SIP transport type to use with this MCU. If the Polycom DMA system's security settings don't allow unencrypted connections, this must be TLS.
Signaling type	Select SIP, H.323, or both, depending on how the Polycom DMA system and MCU are configured.
Enable for conference rooms	Makes the MCU available as a conferencing resource for the Polycom DMA system's Conference Manager. Up to 64 MCUs can be enabled for conference rooms.
ISDN gateway	Makes the MCU available as an ISDN gateway device and enables the <b>ISDN Gateway</b> tab for configuring the gateway.
Class of service	Select to specify the default class of service and the bit rate limits for this MCU. If specified, calls to the MCU use its class of service or the calling endpoint's, whichever is better.
Maximum bit rate (kbps)	Select the maximum bit rate for calls to this MCU.
Minimum downspeed bit rate (kbps)	Select the minimum bit rate to which calls to this MCU can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped. The minimum that applies to a call is the higher of the MCU's and the calling endpoint's.

**Table 6-4** Edit MCU dialog box

Field	Description
<b>ISDN Gateway</b>	
Copy from entry for ISDN gateway	Lets you copy the delimiter and session profiles from another ISDN gateway instead of entering them below. This is especially useful for MGC devices because each ISDN network card must be registered separately, but all cards support the same gateway configuration.
Dial string delimiter	The dial string delimiter used to separate the session profile prefix from the ISDN E.164 number.
Session Profile table	Lists the defined session profile prefixes. A session profile prefix is a numeric dial string prefix that specifies a bit rate for the call and which protocols it supports. Click <b>Add</b> to add a session profile. Click <b>Edit</b> or <b>Delete</b> to change or delete the selected session profile. You can't change or delete session profiles that the gateway registered with, only those that you added.
<b>Media IP Addresses</b>	
Add new media IP address	If you specify the login information for the MCU, the system can get media addresses from the MCU. If not, enter an IP address for media streams and click <b>Add</b> to add it the list below.
Media IP addresses	List of media addresses for the MCU. Click <b>Remove</b> to delete the selected address.
<b>Postliminary</b>	
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 <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

See also:

["MCUs"](#) on page 111

["MCU Procedures"](#) on page 124

["Add Session Profile Dialog Box"](#) on page 123

["Edit Session Profile Dialog Box"](#) on page 123

["Script Debugging Dialog Box for Preliminaries/Postliminaries"](#) on page 215

## Add Session Profile Dialog Box

Lets you add a session profile prefix to the gateway. The following table describes the fields in the dialog box.

**Table 6-5** Add Session Profile dialog box

Field	Description
Session profile	Numeric dial string prefix for this profile.
Bit rate	Bit rate of calls using this profile.
H.320 PSTN H.323 SIP	Select the protocol(s) for this profile. Only H.320 and PSTN are relevant when adding a profile. The other two are selected if the gateway specified them when registering.

See also:

[“Add MCU Dialog Box”](#) on page 117

[“Edit MCU Dialog Box”](#) on page 120

## Edit Session Profile Dialog Box

Lets you edit the selected session profile. You can't edit session profiles that the MCU/gateway registered with, only those that you added.

The following table describes the fields in the dialog box.

**Table 6-6** Add Session Profile dialog box

Field	Description
Session profile	Numeric dial string prefix for this profile.
Bit rate	Bit rate of calls using this profile.
H.320 PSTN H.323 SIP	Select the protocol(s) for this profile. Only H.320 and PSTN are relevant when editing a profile you added. The other two are selected if the gateway specified them when registering.

See also:

[“Add MCU Dialog Box”](#) on page 117

[“Edit MCU Dialog Box”](#) on page 120

## MCU Procedures

### Note

See all the notes in “MCUs” on page 111.

### To view information about an MCU

- 1 Go to **Network > MCU > MCUs**.  
The **MCUs** list appears.
- 2 In the list, select the MCU and in the **Actions** list, click **View Details**.  
The **Device Details** dialog box appears, displaying detailed information about the MCU.

### To add an MCU

- 1 Go to **Network > MCU > MCUs**.
- 2 In the **Actions** list, click **Add**.
- 3 In the **Add MCU** dialog box, complete the editable fields. See “[Add MCU Dialog Box](#)” on page 117.
- 4 To make some of the MCU’s capacity off-limits to the Polycom DMA system (as conferencing resources), set **Video ports reserved for CMA system** and **Voice ports reserved for CMA system** to the values you want to set aside (requires RMX v6.0 and above).  
Use these settings to divide the MCU’s resources between scheduled conferencing (Polycom CMA-controlled) and reservationless conferencing (Polycom DMA-controlled).
- 5 To use a gateway-capable MCU as an ISDN gateway, select the **ISDN Gateway** check box and, on the **ISDN Gateway** tab, specify a dial string delimiter and add one or more session profiles.
- 6 Click **OK**.  
The new MCU appears in the **MCUs** list. If the system is configured as a conferencing resource, it’s placed into service.
- 7 If the MCU is configured as a conferencing resource, add it to the desired MCU pool(s). See “[MCU Pools](#)” on page 127.  
The pool(s) to which the MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used for a conference. See “[MCU Pool Orders](#)” on page 130.



### To edit an MCU

- 1 On the Dashboard, determine whether there are existing calls and conferences on the MCU you want to edit.
- 2 Go to **Network > MCU > MCUs**.
- 3 In the **MCUs** list, select the MCU of interest. If the MCU is being used as a conferencing resource, do the following:
  - a In the **Actions** list, select **Busy Out**. When prompted, confirm.
  - b Wait for any existing calls and conferences to finish.
- 4 In the **Actions** list, click **Edit**.
- 5 In the **Edit MCU** dialog box, edit the fields as required. See [“Edit MCU Dialog Box”](#) on page 120.
- 6 To make more or fewer ports off-limits to the Polycom DMA system, change the **Video ports reserved for CMA system** and **Voice ports reserved for CMA system** values (requires RMX v6.0 and above).
- 7 To use a gateway-capable MCU as an ISDN gateway, select the **Gateway** check box and, on the **Gateway** tab, specify a dial string delimiter and add or change session profiles. To stop using it, clear the **Gateway** check box.
- 8 Click **OK**.

The changes you made appear in the **MCUs** list.
- 9 If the MCU is configured as a conferencing resource, optionally change the MCU pool(s) to which it’s assigned. See [“MCU Pools”](#) on page 127.

The pool(s) to which the MCU belongs, and the pool order(s) to which a pool belongs, are used to determine which MCU is used for a conference. See [“MCU Pool Orders”](#) on page 130.

### To delete an MCU

- 1 On the Dashboard, verify that there are no calls and conferences on the MCU you want to delete.
- 2 Go to **Network > MCU > MCUs**.
- 3 In the **MCUs** list, select the MCU you want to remove from the Polycom DMA system’s pool of available conferencing resources.
- 4 In the **Actions** list, select **Delete**.
- 5 When asked to confirm that you want to delete the selected MCU, click **Yes**.

**To immediately stop using an MCU for conferencing and simplified ISDN dialing**

- 1 Go to **Network > MCU > MCUs**.
- 2 In the **MCUs** list, select the MCU of interest.
- 3 In the **Actions** list, select **Stop Using**.
- 4 When asked to confirm that you want to stop using the MCU, click **Yes**.

The Polycom DMA system immediately terminates all H.323 calls and conferences that it placed on that MCU (for SIP calls only, it migrates the calls to in-service MCUs with available capacity). It also excludes this MCU from consideration for any future conferences and simplified ISDN dialing calls.

This has no effect on the MCU itself, which continues to accept any calls to it from other sources.

**To stop using an MCU, but allow existing calls and conferences to continue**

- 1 Go to **Network > MCU > MCUs**.
- 2 In the **MCUs** list, select the MCU of interest.
- 3 In the **Actions** list, select **Busy Out**.
- 4 When asked to confirm that you want to busy out the MCU, click **Yes**.

The Polycom DMA system stops creating new conferences on that MCU, but it allows its existing conferences to continue and accepts new calls to those conferences. It also excludes this MCU from consideration for simplified ISDN dialing calls.

This has no effect on the MCU itself, which continues to accept any calls to it from other sources.

**To start using an MCU for conferencing and simplified ISDN dialing again**

- 1 Go to **Network > MCU > MCUs**.
- 2 In the **MCUs** list, select the out-of-service MCU of interest.
- 3 In the **Actions** list, select **Start Using**.

See also:

[“MCUs”](#) on page 111

[“Add MCU Dialog Box”](#) on page 117

[“Edit MCU Dialog Box”](#) on page 120

## MCU Pools

The **MCU Pools** list shows the MCU pools, or logical groupings of media servers, that are defined in the Polycom DMA system. In a superclustered system, this list is the same on all clusters in the supercluster. A pool may group MCUs based on location, capability, or some other factor.

### Note

MCU pools were called MCU zones in earlier versions of the Polycom DMA system. The name was changed to avoid confusion with the concept of gatekeeper zones.

The Polycom DMA system uses MCU pools and pool orders to select the MCU on which to host a conference. It's important that you understand how MCU pools and pool orders work, and that you set them up in a way that uses the MCUs in your enterprise effectively as conferencing resources.

Every conference room (VMR) is associated with an MCU pool order (either by direct assignment, via the user's enterprise group membership, or 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. For details of how an MCU is chosen for a conference, see "[MCU Pool Orders](#)" on page 130.

You can use various criteria for organizing MCUs into pools, depending on how you want the MCU resources allocated for conferencing. For instance:

- You could put all MCUs in a specific site or domain into 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.
- You could put one or more MCUs into a pool to be used only by executives, and put that pool into a pool order associated only with those executives' conference rooms.
- You could put MCUs with special capabilities into a pool, and put that pool into a pool order associated only with custom conference rooms requiring those capabilities.

The following table describes the fields in the list.

**Table 6-7** Information in the MCU Pools list

Column	Description
Name	Name of the MCU pool.
Description	Description of the pool, such as the geographic location of the MCUs it contains.
MCUs	The MCUs that are in the pool.

The **Actions** list associated with the **MCU Pools** list contains the items in the following table.

**Table 6-8** *MCU Pools commands*

Command	Description
Add	Opens the <b>Add MCU Pool</b> dialog box, where you can define a new pool.
Edit	Opens the <b>Edit MCU Pool</b> dialog box for the selected pool, where you can change its name, description, and the MCUs it includes.
Delete	Removes the selected MCU pool from the list of pools that are available. A dialog box informs you of the effect on pool orders and asks you to confirm.

See also:

[“Add MCU Pool Dialog Box”](#) on page 128

[“Edit MCU Pool Dialog Box”](#) on page 129

[“MCU Pool Procedures”](#) on page 129

## Add MCU Pool Dialog Box

Lets you define a new MCU pool in the DMA system. The following table describes the fields in the dialog box.

**Table 6-9** *Add MCU Pool dialog box*

Field	Description
Name	Name of the MCU pool.
Description	Description of the pool. This should be something meaningful, such as the geographic location of the MCUs that the pool contains.
Available MCUs	Lists the MCUs available to the Polycom DMA system.
Selected MCUs	Lists the MCUs included in the pool. The arrow buttons move MCUs from one list to the other.

See also:

[“MCU Pools”](#) on page 127

[“MCU Pool Procedures”](#) on page 129

## Edit MCU Pool Dialog Box

Lets you edit an MCU pool. The following table describes the fields in the dialog box.

**Table 6-10** *Edit MCU Pool dialog box*

Field	Description
Name	Name of the MCU pool.
Description	Brief description of the pool. This should be something meaningful, such as the geographic location of the MCUs that the pool contains.
Available MCUs	Lists the MCUs available to the Polycom DMA system.
Selected MCUs	Lists the MCUs included in the pool. The arrow buttons move MCUs from one list to the other.

See also:

[“MCU Pools”](#) on page 127

[“MCU Pool Procedures”](#) on page 129

## MCU Pool Procedures

### To view the MCU Pools list

>> Go to **Network > MCU > MCU Pools**.

The **MCU Pools** list appears.

### To add an MCU Pool

- 1 Go to **Network > MCU > MCU Pools**.
- 2 In the **Actions** list, click **Add**.
- 3 In the **Add MCU Pool** dialog box, complete the editable fields. All are required. See [“Add MCU Pool Dialog Box”](#) on page 128.
- 4 Click **OK**.

The new MCU pool appears in the **MCU Pools** list. The MCUs included in the pool are displayed.

### To edit an MCU Pool

- 1 Go to **Network > MCU > MCU Pools**.
- 2 In the **MCU Pools** list, select the pool, and in the **Actions** list, click **Edit**.

**3** In the **Edit MCU Pool** dialog box, edit the fields as required. See [“Edit MCU Pool Dialog Box”](#) on page 129.

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

The changes you made appear in the **MCU Pools** list.

#### To delete an MCU Pool

**1** Go to **Network > MCU > MCU Pools**.

**2** In the **MCU Pools** list, select the MCU pool you want to remove.

**3** In the **Actions** list, select **Delete**.

If the pool is included in one or more pool orders, the system warns you and provides information about the consequences of deleting it.

**4** When asked to confirm that you want to delete the selected MCU pool, click **Yes**.

See also:

[“MCU Pools”](#) on page 127

[“Add MCU Pool Dialog Box”](#) on page 128

[“Edit MCU Pool Dialog Box”](#) on page 129

## MCU Pool Orders

The **MCU Pool Orders** list shows the MCU pool orders that are defined in the Polycom DMA system. In a superclustered system, this list is the same on all clusters in the supercluster. A pool order contains one or more MCU pools and specifies the order of preference in which the pools are used.

#### Note

MCU pools were called MCU zones in earlier versions of the Polycom DMA system. The name was changed to avoid confusion with the concept of gatekeeper zones.

The Polycom DMA system uses MCU pools and pool orders to select the MCU on which to host a conference. It's important that you understand how MCU pools and pool orders work, and that you set them up in a way that uses the MCUs in your enterprise effectively as conferencing resources.

Every conference room (VMR) is associated with an MCU pool order in one of the following ways:

- By direct assignment. See [“Edit Conference Room Dialog Box”](#) on page 284.
- 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. For some examples of how MCUs can be organized into pools for specific purposes, see “[MCU Pools](#)” on page 127.

The Polycom DMA system chooses an MCU for a user 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 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.

If there are multiple MCUs that are equally capable, select the least used.
- 4 If no MCUs in the selected MCU pool have capacity, select the next MCU pool in the pool order and return to step 3.
- 5 If no MCUs are available in any of the MCU pools:
  - If fallback is enabled, select the best MCU available to the Polycom DMA system, based on the system’s capability algorithm.
  - If fallback is not enabled, reject the call.

The following table describes the fields in the list.

**Table 6-11** Information in the MCU Pool Orders list

Column	Description
Priority	Priority ranking of the pool order.
Name	Name of the pool order.
Description	Brief description of the pool order.
MCU Pools	The MCU pools that are in the pool order.
Fallback	Indicates whether this pool order is set to fall back to any available MCU if there are no available MCUs in its pools.

The **Actions** list associated with the **MCU Pool Orders** list contains the items in the following table.

**Table 6-12** *MCU Pool Orders commands*

Command	Description
Add	Opens the <b>Add MCU Pool Order</b> dialog box, where you can define a new pool order.
Edit	Opens the <b>Edit MCU Pool Order</b> dialog box for the selected pool order, where you can change its name, description, the MCU pools it includes, and their priority order.
Delete	Removes the selected MCU pool order from the list of pool orders that are available. A dialog box asks you to confirm.
Move Up	Increases the priority ranking of the selected pool order.
Move Down	Decreases the priority ranking of the selected pool order.

See also:

[“Add MCU Pool Order Dialog Box”](#) on page 132

[“Edit MCU Pool Order Dialog Box”](#) on page 133

[“MCU Pool Order Procedures”](#) on page 133

[“Enterprise Groups Procedures”](#) on page 287

## Add MCU Pool Order Dialog Box

Lets you define a new MCU pool order in the DMA system. The following table describes the fields in the dialog box.

**Table 6-13** *Add MCU Pool Order dialog box*

Field	Description
Name	Name of the MCU pool order.
Description	Brief description of the pool order.
Available MCU pools	Lists the MCU pools available to the system.
Selected MCU pools	Lists the pools included in the pool order in their priority order. The left/right arrow buttons move pools in and out of the list. The up/down arrow buttons change the priority rankings of the pools.
Fall back to any available MCU	Indicates whether this pool order is set to use any available MCU if there is no available MCU in its pools.



See also:

[“MCU Pool Orders”](#) on page 130

[“MCU Pool Order Procedures”](#) on page 133

## Edit MCU Pool Order Dialog Box

Lets you edit an MCU pool order. The following table describes the fields in the dialog box.

**Table 6-14** *Edit MCU Pool Order dialog box*

Field	Description
Name	Name of the MCU pool order.
Description	Brief description of the pool order.
Available MCU pools	Lists the MCU pools available to the Polycom DMA system.
Selected MCU pools	Lists the pools included in the pool order in their priority order. The left/right arrow buttons move pools from one list to the other. The up/down arrow buttons change the priority rank of the selected pool.
Fall back to any available MCU	Indicates whether this pool order is set to use any available MCU if there is no available MCU in its pools.

See also:

[“MCU Pool Orders”](#) on page 130

[“MCU Pool Order Procedures”](#) on page 133

## MCU Pool Order Procedures

### To view the MCU Pool Orders list

>> Go to **Network > MCU > MCU Pool Orders**.

The **MCU Pool Orders** list appears.

### To add an MCU Pool Order

- 1 Go to **Network > MCU > MCU Pool Orders**.
- 2 In the **Actions** list, click **Add**.
- 3 In the **Add MCU Pool** dialog box, complete editable fields. All are mandatory. See [“Add MCU Pool Dialog Box”](#) on page 128.

- 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.

#### **To edit an MCU Pool Order**

- 1 Go to **Network > MCU > 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 box, edit the fields as required. See [“Edit MCU Pool Dialog Box”](#) on page 129.
- 4 Click **OK**.

The changes you made appear in the **MCU Pool Orders** list.

#### **To delete an MCU Pool Order**

- 1 Go to **Network > MCU > MCU Pool Orders**.
- 2 In the **MCU Pool Orders** list, select the pool order, and in the **Actions** list, select **Delete**.
- 3 When asked to confirm that you want to delete the selected MCU, click **Yes**.

See also:

[“MCU Pool Orders”](#) on page 130

[“Add MCU Pool Order Dialog Box”](#) on page 132

[“Edit MCU Pool Order Dialog Box”](#) on page 133

---

# Integrations with Other Systems

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system configuration topics related to integrating the system with external systems:

- [Microsoft Active Directory Integration](#)
- [Microsoft Exchange Server Integration](#)
- [Polycom CMA System Integration](#)
- [Juniper Networks SRC Integration](#)

## Microsoft Active Directory Integration

When you integrate the Polycom DMA system with your Microsoft Active Directory, the enterprise users (Active Directory members) become Conferencing Users in the Polycom 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 Polycom DMA system reads the directory information nightly to update the user and group information in its cache. You can force a cache refresh at any time using the **Update** button. Between updates, it accesses the directory only to authenticate login passwords.

In a superclustered environment, one cluster is responsible for integrating with Active Directory and updating the cache nightly, and the cache is available to all clusters through the replicated shared data store. The other clusters connect to Active Directory only to authenticate user credentials.

**Note**

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments.

UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Lync Server 2010 or Office Communications Server integrations. Please see:

[http://www.polycom.com/services/professional\\_services/index.html](http://www.polycom.com/services/professional_services/index.html)

Or contact your local Polycom representative for more information.

If the Active Directory is on Windows Server 2008 R2 and AD integration fails, see:

<http://support.microsoft.com/kb/977180>

See also:

[“Microsoft Active Directory Page”](#) on page 137

[“Active Directory Integration Procedure”](#) on page 141

[“Understanding Base DN”](#) on page 145

[“Adding Passcodes for Enterprise Users”](#) on page 146

[“About the System’s Directory Queries”](#) on page 148

[“Active Directory Integration Report”](#) on page 349

[“Conference Room Errors Report”](#) on page 353





[“Groups”](#) on page 284

[“Enterprise Groups Procedures”](#) on page 287

## Microsoft Active Directory Page

The following table describes the fields on the **Microsoft Active Directory** page.

**Table 7-1** Fields on the Microsoft Active Directory page

Field	Description
Enable integration with Microsoft Active Directory® Server	Enables the Active Directory integration fields and the <b>Update</b> button, which initiates a connection to the Microsoft Active Directory.
<b>Connection Status</b>	
<node name and icons>	<p>The Polycom DMA system node(s) and one or more of the following status icons for each:</p> <p> Warning – Appears only if an error has occurred. Hover over it to see a description of the problem or problems.</p> <p> Connected – This is real-time status. The system connects to the Active Directory every 5 seconds while this page is displayed.</p> <p> Disconnected – The system either isn't integrated with Active Directory or is unable to connect.</p> <p> Encrypted – Appears only if the connection to the directory is encrypted.</p>
Status	<p><b>OK</b> indicates that the node successfully connected to the Active Directory. If it didn't, an error message appears.</p> <p>If you're an administrator, this label is a link to the <a href="#">Active Directory Integration Report</a>.</p>
User and group cache	Shows the state of the node's cache of directory data and when it was last updated.
Total users/rooms	<p>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.</p> <p><b>Note:</b> If you don't specify an Active Directory attribute for conference room ID generation, the number of rooms is zero.</p>

**Table 7-1** Fields on the Microsoft Active Directory page (continued)

Field	Description
Conference room errors	<p>Number of enterprise users for whom conference rooms couldn't be generated.</p> <p>If you're an administrator, this label is a link to the <a href="#">Conference Room Errors Report</a> report.</p> <p><b>Note:</b> If you don't specify an Active Directory attribute for conference room ID generation, the number of errors equals the number of users.</p>
Orphaned users/groups	<p>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).</p> <p>If you're an administrator, this label is a link to the <a href="#">Orphaned Groups and Users Report</a>.</p>
Enterprise passcode errors	<p>Number of enterprise users for whom passcodes were generated that aren't valid.</p> <p>If you're an administrator, this label is a link to the <a href="#">Enterprise Passcode Errors Report</a>.</p>
<b>Active Directory Connection</b>	
Auto-discover from FQDN	<p>If this option is selected, the system uses serverless bind to find the closest global catalog servers. Enter the DNS domain name. We strongly recommend using this option.</p> <p>If the system can't determine the site to which it belongs, it tries to connect to any global catalog server.</p> <p>If that fails, it uses the entered DNS domain name as a host name and continues as if the <b>IP address or host name</b> option were selected.</p> <p>The system's <a href="#">Network Settings</a> setup must have at least one domain name server specified.</p> <p>Check the <a href="#">Active Directory Integration Report</a> to see whether serverless bind succeeded and what the site name is.</p>
IP address or host name	<p>If this option is selected, the system attempts to connect to the Microsoft Active Directory domain controller specified.</p> <p>For a single-domain forest, enter the host name or IP address of a domain controller.</p> <p>For a multi-domain forest, we don'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.</p> <p>The Polycom 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.</p>

**Table 7-1** Fields on the Microsoft Active Directory page (continued)

Field	Description
Domain\user name	<p>LDAP service account user ID for system access to the Active Directory. Must be set up in the Active Directory, but should not have Windows login privileges.</p> <p><b>Note:</b> If you use Active Directory attributes that aren't 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.</p> <p>The Polycom DMA system initially assigns the Administrator user role to this user (see <a href="#">"User Roles Overview"</a> on page 265), so you can use this account to give administrative access to other enterprise user accounts.</p> <p><b>Caution:</b> Leaving a user role assigned to this account represents a <b>serious security risk</b>. For best security, remove the Administrator user role so that it can't be used for logging into the Polycom DMA system management interface.</p>
Password	Login password for service account user ID.
User LDAP filter	<p>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.</p> <p>Don't edit this expression unless you understand LDAP filter syntax. See RFC 2254 for syntax information.</p>
Base DN	<p>Can be used to restrict the Polycom 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, All Domains, initially. See <a href="#">"Understanding Base DN"</a> on page 145.</p>
Time of day to refresh cache	Time at which the Polycom DMA system should log into the directory server(s) and update its cache of user and group data.
Territory	<p>Specifies the territory whose Polycom DMA system cluster is responsible for updating the user and group data cache.</p> <p>In a superclustered system, this information is shared across the supercluster. The other clusters access the directory only to authenticate passwords. See <a href="#">"Territories"</a> on page 257 for more information.</p>

**Table 7-1** Fields on the Microsoft Active Directory page (continued)

Field	Description
<b>Enterprise Conference Room ID Generation</b>	
Directory attribute	<p>The name of the Active Directory attribute from which the Polycom DMA system should derive conference room IDs (virtual meeting room numbers). Generally, organizations use a phone number field for this.</p> <p>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 isn't in the Global Catalog, the system queries each domain controller for the data.</p> <p>Leave this field blank if you don't want the system to create conference rooms for the enterprise users.</p>
Characters to remove	<p>Characters that might need to be stripped from a phone number field's value to ensure a numeric conference room ID.</p> <p>The default string includes \t, which represents the tab character. Use \ to remove backslash characters.</p>
Maximum characters used	<p>Desired length of conference room IDs. The Polycom DMA system strips excess characters from the beginning, not the end. If you specify 7, the room IDs will contain the last 7 valid characters from the Active Directory attribute being used.</p>
<b>Enterprise Chairperson and Conference Passcode Generation</b>	
Chairperson directory attribute	<p>The name of the Active Directory attribute that contains the chairperson passcodes. In choosing an attribute, remember that passcodes must be numeric.</p> <p>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 isn't in the Global Catalog, the system queries each domain controller for the data.</p> <p>Leave this field blank if you don't want the system to create chairperson passcodes for the enterprise users.</p>
Maximum characters used	<p>Desired length of chairperson passcodes. The Polycom DMA system strips excess characters from the beginning, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.</p>



**Table 7-1** Fields on the Microsoft Active Directory page (continued)

Field	Description
Conference directory attribute	<p>The name of the Active Directory attribute that contains the conference passcodes. In choosing an attribute, remember that passcodes must be numeric.</p> <p>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 isn't in the Global Catalog, the system queries each domain controller for the data.</p> <p>Leave this field blank if you don't want the system to create conference passcodes for the enterprise users.</p>
Maximum characters used	<p>Desired length of conference passcodes. The Polycom DMA system strips excess characters from the beginning, not the end. If you specify 7, the passcodes will contain the last 7 numeric characters from the Active Directory attribute being used.</p>

See also:

- [“Microsoft Active Directory Integration”](#) on page 135
- [“Active Directory Integration Procedure”](#) on page 141
- [“Understanding Base DN”](#) on page 145
- [“Adding Passcodes for Enterprise Users”](#) on page 146
- [“About the System’s Directory Queries”](#) on page 148

## Active Directory Integration Procedure

Before performing the procedure below, read [“Set Up Security”](#) on page 21 and [“Connect to Microsoft Active Directory”](#) on page 23. You should also have a good idea of how many enterprise users you expect the system to retrieve.

### To integrate with Active Directory

- 1 In Windows Server, add the service account (read-only user account) that the Polycom DMA system will use to read the Active Directory. Configure this account as follows:
  - User can't change password.
  - Password never expires.
  - User can only access services on the domain controllers and cannot log in anywhere.

**Note**

If you have a Polycom CMA system, be aware that the machine account used for AD integration by the CMA system and the service account used for AD integration by the DMA system have different requirements. Don't try to use the same account for both purposes. In particular, the whitelist of machines that the Polycom CMA system is allowed to log into should contain only the CMA system, while the whitelist of machines the Polycom DMA system is allowed to log into should contain only the domain controllers.

If you use Active Directory attributes that aren't replicated across the enterprise via the Global Catalog server mechanism, the system must query each domain for the data. Make sure that the whitelist for this service account is correct and that it can connect to all the LDAP servers in each domain.

- 2 In the Polycom DMA system, replace the default local administrative user with your own user account that has the same user roles. See [“Users Procedures”](#) on page 280.
- 3 Log into the Polycom DMA system as the local user you created in step 2 and go to **Admin > Integrations > Microsoft Active Directory**.
- 4 Check **Enable integration with Microsoft® Active Directory Server** and complete the information in the **Active Directory Connection** section.
  - a Unless you have a single domain environment and no global catalog, select **Auto-discover from FQDN** and enter the DNS domain name.

**Note**

We don't recommend using the **IP address or host name** option in a multi-domain environment. If you must, enter the host name or IP address of a specific global catalog server, not the DNS domain name.

- b For **Domain\user name**, enter the domain and user ID of the account you created in step 1.
  - c Leave **Base DN** set to the default, *All Domains*. Don't edit the **User LDAP filter** expression unless you understand LDAP filter syntax (see RFC 2254) and know what changes to make.
  - d Specify the time each day that you want the Polycom DMA system to check the Active Directory for changes.
  - e Select the territory whose cluster should perform the integration and daily updates.
- 5 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 Specify the Active Directory attribute from which to generate room IDs.

Your users will be happier if room IDs are numeric and not longer than necessary to ensure uniqueness. Phone numbers are the most likely choice, or maybe 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 number of characters to use.

After the system strips out characters to remove, it removes characters in excess of this number from the beginning of the string.

#### Note

Leave the **Enterprise Chairperson and Conference Passcode Generation** section alone for now. Once the system is integrated successfully, if you want to add passcode support, see [“Adding Passcodes for Enterprise Users”](#) on page 146.

- 6 Click **Update**.

After a short time, the system confirms that Active Directory configuration has been updated.

- 7 Note the time. Click **OK**.

- 8 To restrict the Polycom 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 4-6, selecting the value you want from those now available in the **Base DN** list. See [“Understanding Base DN”](#) on page 145.

- 9 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).

- 10 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. The service account user ID specified in step 4b lets you do so initially.

- b Go to **User > Users**, locate your named enterprise account, and give it Administrator privileges. See [“User Roles Overview”](#) on page 265 and [“Users Procedures”](#) on page 280.

- c Log out and log back in using your named enterprise account.

- d Secure the service account by removing all user roles in the Polycom DMA system. See [“Edit User Dialog Box”](#) on page 272.

**Caution**

Leaving user roles assigned to the service account represents a **serious security risk**. For best security, remove all user roles so that this account can't be used for logging into the Polycom DMA system management interface.

- 11** If, in step 9, 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 aren't.
  - 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.

**Note**

If you're not familiar with LDAP filter syntax (as defined in RFC 2254) and knowledgeable about enterprise directories in general and your specific implementation in particular, please consult with someone who is.

- 12** If, in step 9, 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 last completed step 4.
  - 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.
- 13** If necessary, repeat steps 4-9 and steps 11 and/or 12, modifying the integration parameters as needed, until you get a satisfactory result.

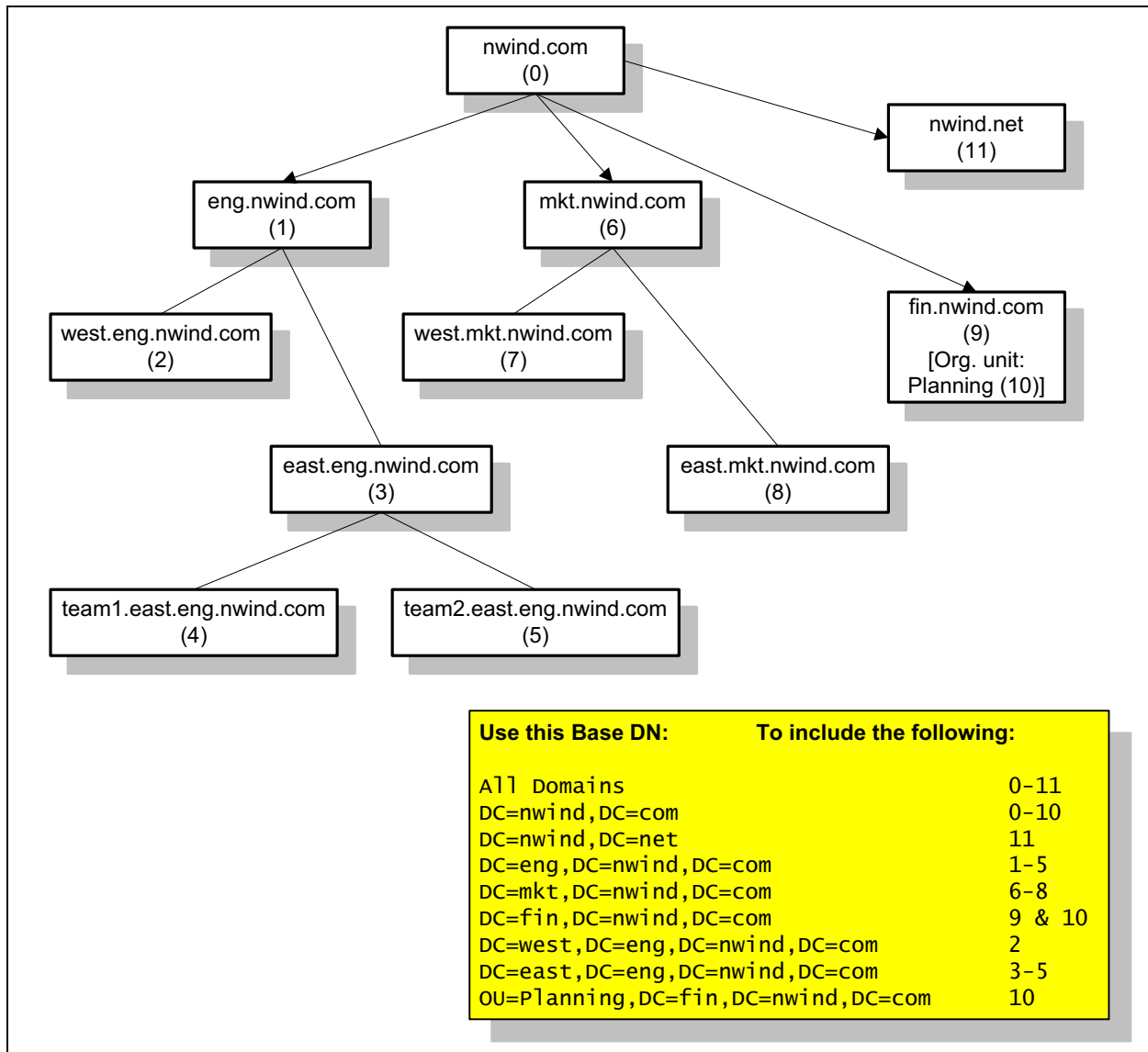
See also:

- ["Microsoft Active Directory Integration"](#) on page 135
- ["Understanding Base DN"](#) on page 145
- ["Adding Passcodes for Enterprise Users"](#) on page 146
- ["About the System's Directory Queries"](#) on page 148
- ["Active Directory Integration Report"](#) on page 349
- ["Conference Room Errors Report"](#) on page 353
- ["Groups"](#) on page 284
- ["Enterprise Groups Procedures"](#) on page 287

## 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 Polycom DMA system. It acts like a filter.

The diagram below 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 AD 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.

See also:

[“Microsoft Active Directory Integration”](#) on page 135

[“Active Directory Integration Procedure”](#) on page 141

[“About the System’s Directory Queries”](#) on page 148

## Adding Passcodes for Enterprise Users

Polycom RMX MCUs provide two optional security features for conferences, which the Polycom DMA system fully supports:

- **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 conference chairpersons. Chairpersons have additional privileges, such as controlling recording. A conference can be configured to not start until a chairperson joins and to end when the last chairperson leaves (see [“Add Conference Template Dialog Box”](#) on page 170).

### Note:

If Cisco (formerly Tandberg) Codian MCUs are included in the Polycom 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 Polycom 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 Polycom 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.

### To generate chairperson and conference passcodes for enterprise users

- 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. But if the attributes you select aren't available in the Global Catalog, the system can read them directly from each domain.

#### Note

You could use an existing attribute that contains numeric data, such as an employee ID. This may not provide much security, but might be sufficient for conference passcodes.

- 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 Polycom DMA system, go to **Admin > 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. 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 when you last completed step 6.
  - 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.

**Note**

Unless users have already been provisioned with passcodes in your Active Directory or you're using an existing attribute, most users will probably not have passcodes assigned. Duplicate and invalid passcodes should be your main concern because they could indicate a problem with the type of data in the selected attributes or with the number of characters you elected to use.

See also:

[“Microsoft Active Directory Integration”](#) on page 135

[“Microsoft Active Directory Page”](#) on page 137

[“Active Directory Integration Procedure”](#) on page 141

[“Active Directory Integration Report”](#) on page 349

## About the System's Directory Queries

The Polycom DMA system uses the following subtree scope LDAP queries. In a standard AD configuration, all these queries use indexes.

- [User Search](#)
- [Group Search](#)
- [Global Group Membership Search](#)
- [Attribute Replication Search](#)
- [Configurable Attribute Domain Search](#)
- [Domain Search](#)
- [Service Account Search](#)

The system runs the first three queries every time it creates or updates its cache:

- When you click **Update** on the **Microsoft Active Directory** page
- When the system restarts (if integrated with the Active Directory)
- At the scheduled daily cache refresh time

The elements in italics are examples. The actual values of these variables depend on your configuration.



## User Search

This search queries the global catalog. In a standard AD 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**. See ["Understanding Base DN"](#) on page 145.

- 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. See ["Microsoft Active Directory Integration"](#) on page 135.

- Index used: idx\_objectCategory:32561:N

The search used this index in our testing environment, using a standard AD 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.

See ["Microsoft Active Directory Integration"](#) on page 135 and ["Adding Passcodes for Enterprise Users"](#) on page 146.

## Group Search

This search queries the global catalog. In a standard AD 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**. See ["Understanding Base DN"](#) on page 145.

- Filter: (&(objectClass=group)(|(groupType=-2147483640)(groupType=-2147483646)))

- Indexes used: idx\_groupType:6675:N;idx\_groupType:11:N

The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- Attributes returned: cn, description, sAMAccountName, groupType, member

## Global Group Membership Search

This 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**. See "[Understanding Base DN](#)" on page 145.

- Filter: (&(objectClass=group)(groupType=-2147483646))
- Index used: idx\_groupType:6664:N

The search used this index in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- Attributes returned: member

## Attribute Replication Search

This 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 purpose of this query is simply to determine if those Active Directory attributes are replicated to the global catalog. If they are, the [User Search](#) retrieves them. If any of them isn't, 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: (|(LDAPDisplayName=telephoneNumber)(LDAPDisplayName=chairpasscode)(LDAPDisplayName=confpasscode))

The filter variables depend on the configurable Active Directory attributes specified in the **Enterprise Conference Room ID Generation** and

**Enterprise Chairperson and Conference Passcode Generation** sections (any of these that's empty is omitted from the filter).

- Indexes used: `idx_LDAPDisplayName:3:N;idx_LDAPDisplayName:2:N;idx_LDAPDisplayName:1:N`

The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- Attributes returned: `LDAPDisplayName, isMemberOfPartialAttributeSet`

## Configurable Attribute Domain Search

This 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 [User Search](#)
- Index used: same as in [User Search](#)
- Attributes returned: `SAMAccountName`, attribute(s) not in global catalog

## Domain Search

This 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). See "[Active Directory Integration Report](#)" on page 349.

- Filter: `(&(objectCategory=crossRef)(systemFlags=3))`
- Indexes used: `idx_objectCategory:11:N`

The search used these indexes in our testing environment, using a standard AD configuration (no indexes added). Results may be different for a different configuration.

- Attributes returned: `cn, dnsRoot, nCName`

## Service Account Search

This search queries the global catalog. In a standard AD 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**. See ["Understanding Base DN"](#) on page 145.

- 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. See ["Microsoft Active Directory Integration"](#) on page 135. The second variable depends on the value entered in the **Service account ID** field on the **Microsoft Active Directory** page. See ["Microsoft Active Directory Integration"](#) on page 135.

- Index used: idx\_objectCategory:32561:N

The search used this index in our testing environment, using a standard AD 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

See also:

["Microsoft Active Directory Integration"](#) on page 135

["Microsoft Active Directory Page"](#) on page 137

["Active Directory Integration Procedure"](#) on page 141

["Understanding Base DN"](#) on page 145

## Microsoft Exchange Server Integration

On the **Microsoft Exchange Server** page, you can integrate the Polycom DMA system with your Microsoft Exchange Server, enabling users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.

### Note

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners to help customers successfully design, deploy, optimize, and manage Polycom visual communication within their third-party UC environments.

UC Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Lync Server 2010 or Office Communications Server integrations. Please see:

[http://www.polycom.com/services/professional\\_services/index.html](http://www.polycom.com/services/professional_services/index.html)

Or contact your local Polycom representative for more information.

Exchange Server integration can't be enabled, and the Polycom DMA system doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook, in **Maximum security** mode. See "[The Consequences of Enabling Maximum Security Mode](#)" on page 45.

As with other Outlook meeting requests, the meeting organizer invites attendees and specifies where and when to meet. "Where" in this case is a conference room, or virtual meeting room (VMR), on the Polycom DMA system. The VMR number is generated by the add-in.

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 (Microsoft Office Communicator or Polycom CMA 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 Polycom DMA system monitors that mailbox and accepts or declines the invitations received.

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 isn't in the Polycom DMA system's Active Directory cache.

- The invitation contains invalid or incomplete meeting data (the machine-readable metadata block at the bottom of the invitation labeled “POLYCOM VMR ENCODED TOKEN” and preceded with a warning not to edit).
- The meeting’s duration exceeds the system’s **Conference Duration** setting (see [“Conference Settings”](#) on page 163).
- The conference or chairperson passcode is not valid (see [“Adding Passcodes for Enterprise Users”](#) on page 146).

**Note**

Calendaring is not 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 aren’t declined due to lack of resources.

This version of the Polycom 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 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 DMA system is part of the Polycom Conferencing for Outlook solution.

See also:

[“Integrations with Other Systems”](#) on page 135

[“Microsoft Exchange Server Page”](#) on page 155

[“Exchange Server Integration Procedure”](#) on page 155

## Microsoft Exchange Server Page

The following table describes the fields on the **Microsoft Exchange Server** page.

**Table 7-2** Fields on the Microsoft Exchange Server page

Field	Description
Enable integration with Microsoft® Exchange Server	Enables the Exchange server integration fields and the <b>Update</b> button, which initiates a connection to Microsoft Exchange server.
Exchange Server address	Fully qualified domain name (FQDN) or IP address of the Exchange server.
Domain\user name	The user ID for the Polycom Conferencing infrastructure mailbox on the Exchange server.
Password	The password for the Polycom Conferencing user ID.
Territory	Select a territory, thereby determining which Polycom DMA cluster is responsible for integrating with the Exchange server and monitoring the Polycom Conferencing infrastructure mailbox. See <a href="#">“Territories”</a> on page 257 for more information.
Accept Exchange notifications from these additional IP addresses	If you have multiple Exchange servers behind a load balancer, specify the IP address of each individual Exchange server.

See also:

[“Microsoft Exchange Server Integration”](#) on page 153

[“Exchange Server Integration Procedure”](#) on page 155

## Exchange Server Integration Procedure

### To integrate the Polycom DMA system with your Exchange server

#### Note

Unless the **Allow unencrypted calendar notifications from Exchange server** security option is enabled (see [“Security Settings”](#) on page 41), the Polycom 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 status (see Dashboard) remains **Subscription pending** indefinitely, the Polycom DMA system does not receive calendar notifications, and incoming meeting request messages are only processed approximately every 4 minutes.

- 1 Confirm that the Polycom DMA system has been successfully integrated with your Active Directory (see “[Integrations with Other Systems](#)” on page 135) and verify the domain.

Successful calendar integration requires that the Polycom DMA system be integrated with Microsoft Active Directory.

- 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 Polycom 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.

#### Caution

Create a dedicated Polycom Conferencing mailbox that’s used ***specifically and exclusively*** for the purpose of receiving Polycom Conferencing meeting invitations. This is important because the Polycom DMA system will delete all messages from the Inbox when it checks this mailbox for meeting invitations.

When creating the user ID for the system, be sure to specify the same domain used to integrate with the Active Directory. Specify the Display Name as you want it to appear in the To field of invitations. We recommend using Polycom Conference (first and last name respectively).

- 4 Go to **Admin > Integrations > Microsoft Exchange Server**.
- 5 Check **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 DMA cluster to be responsible for calendaring.
- 8 If you have multiple Exchange servers behind a load balancer, under **Accept Exchange notifications from these additional IP addresses**, add the IP address of each individual Exchange server.
- 9 Click **Update**.  
A dialog box 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 to be distributed to your users (see the online help for the Add-in). 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®*).

See also:

[“Microsoft Exchange Server Integration”](#) on page 153

[“Microsoft Exchange Server Page”](#) on page 155

## Polycom CMA System Integration

Integrating with a Polycom CMA system provides the Polycom DMA system with site topology information and user-to-device association information. Both kinds of information can be manually configured on the Polycom DMA system, without integrating with the Polycom CMA system. Integrating with the Polycom CMA system ensures consistency.

While the Polycom DMA system is integrated with the Polycom CMA system, site topology and user-to-device association may only be configured on the Polycom CMA system. If the integration is terminated, the Polycom DMA system retains the information last obtained from the CMA system, but it becomes editable.

The Polycom DMA system uses site topology information for a variety of purposes, including cascading of conferences, bandwidth management, and Session Border Controller selection. See [“Add Conference Template Dialog Box”](#) on page 170 and [“About the Call Server Capabilities”](#) on page 203.

The Polycom DMA system uses user-to-device association to assign classes of service to endpoints based on the user they belong to. See [“Associate User Dialog Box”](#) on page 80.

Your DNS servers must be able to resolve the Polycom DMA system’s FQDN to its virtual IP address. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

In addition, the DNS servers must be able to resolve Polycom CMA system’s FQDN to its IP address. This is necessary even if you specify the Polycom CMA system’s IP address when you join it.

**Note**

CMA integration is not supported in **Maximum security** mode. See [“The Consequences of Enabling Maximum Security Mode”](#) on page 45.

If you want to support cascading, but don't have a Polycom CMA system, you must create site topology information on the Polycom DMA system. See [“Site Topology”](#) on page 241.

The cascade links between RMX MCUs must use H.323 signaling. For conferences with cascading enabled, the Polycom 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 Polycom DMA system are also configured for SIP signaling).

See also:

[“Integrations with Other Systems”](#) on page 135

[“Polycom CMA System Page”](#) on page 158

[“Join CMA Dialog Box”](#) on page 159

[“Polycom CMA System Integration Procedures”](#) on page 160

## Polycom CMA System Page

The **Polycom CMA System** page contains the **Join CMA** command, which you use to integrate with your Polycom CMA system. When the system is integrated with a Polycom CMA system, it contains the **Leave CMA** command, which you use to terminate the integration.

The list on this page displays information about the Polycom CMA system. The following table describes the fields in the list.

**Table 7-3** Fields in the Polycom CMA System list

Field	Description
Host name	Name of the system.
IP Address	IP address of the system.
Model	Type of system (CMA 4000 or 5000).
Version	Software version of the system.
Status	Status of last attempt to contact system (OK or Unreachable).
Time	Time of last attempt to contact system.

See also:

[“Integrations with Other Systems”](#) on page 135

[“Polycom CMA System Integration”](#) on page 157

[“Join CMA Dialog Box”](#) on page 159

[“Polycom CMA System Integration Procedures”](#) on page 160

## Join CMA Dialog Box

Lets you integrate the Polycom DMA system with a Polycom CMA system to obtain site topology information and user-to-device association information.

### Note

CMA integration is not supported in **Maximum security** mode. See [“The Consequences of Enabling Maximum Security Mode”](#) on page 45.

### Note

Your DNS servers must be able to resolve the Polycom DMA system’s FQDN to its virtual IP address. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

In addition, the DNS servers must be able to resolve the Polycom CMA system’s FQDN to its IP address. This is necessary even if you specify the Polycom CMA system’s IP address when you join it.

The following table describes the fields in the dialog box.

**Table 7-4** *Fields in the Join CMA dialog box*

Field	Description
Host name or IP address	The Polycom CMA system with which to integrate.
User name	Administrative user ID with which the Polycom DMA system can log into the Polycom CMA system.
Password	Password for the administrative user ID.

See also:

[“Integrations with Other Systems”](#) on page 135

[“Polycom CMA System Integration”](#) on page 157

[“Polycom CMA System Page”](#) on page 158

[“Polycom CMA System Integration Procedures”](#) on page 160

## Polycom CMA System Integration Procedures

### Note

CMA integration is not supported in **Maximum security** mode. See [“The Consequences of Enabling Maximum Security Mode”](#) on page 45.

### Note

Your DNS servers must be able to resolve the Polycom DMA system’s FQDN to its virtual IP address. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

In addition, the DNS servers must be able to resolve the Polycom CMA system’s FQDN to its IP address. This is necessary even if you specify the Polycom CMA system’s IP address when you join it.

### To integrate with a Polycom CMA system

- 1 Go to **Admin > Integrations > Polycom CMA System**.
- 2 In the **Actions** list, select **Join CMA**.
- 3 In the **Join CMA** dialog box, enter the host name or IP address of the Polycom CMA system and the credentials with which to log into it. Then click **OK**.
- 4 When asked to confirm that you want to join, click **Yes**.

The system connects to the Polycom CMA system, establishes the integration, and obtains site topology and user-to-device association data (this may take a few minutes). A dialog box informs you when the process is complete.

- 5 On the **Polycom CMA System** page, verify the CMA integration information.
- 6 Go to **Network > Site Topology > Sites**, and from there to the other site topology pages, to see the site topology information obtained from the Polycom CMA system.

### To terminate the integration with a Polycom CMA system

- 1 Go to **Admin > Integrations > Polycom CMA System**.
- 2 In the **Actions** list, select **Leave CMA**.
- 3 When asked to confirm that you want to leave, click **Yes**.

The system connects to the Polycom CMA system and terminates the integration. A dialog box informs you when the process is complete.

- 4** On the **Polycom CMA System** page, verify that the system is no longer integrated with the Polycom CMA system.

The Polycom DMA system retains the site topology and user-to-device association information last obtained from the CMA system, but it's now editable.

See also:

[“Integrations with Other Systems”](#) on page 135

[“Polycom CMA System Integration”](#) on page 157

[“Polycom CMA System Page”](#) on page 158

[“Join CMA Dialog Box”](#) on page 159

## Juniper Networks SRC Integration

You can integrate the Polycom DMA system's Call Server with a Juniper Networks SRC Series Session and Resource Control module to provide bandwidth assurance services.

See also:

[“Integrations with Other Systems”](#) on page 135

[“Juniper Networks SRC Page”](#) on page 161

[“Juniper Networks SRC Integration Procedure”](#) on page 162

## Juniper Networks SRC Page

The following table describes the fields on the **Juniper Networks SRC** page.

**Table 7-5** Fields on the Juniper Networks SRC page

Field	Description
Enable integration with Juniper Networks® SRC	Enables the SRC integration fields and the <b>Update</b> button, which initiates a connection to the Juniper Networks SRC server.
IP address or host name	The host name or IP address of the SRC server.
Server port	The port number that the Polycom DMA system uses to connect to the SRC server.
Client ID	The user ID with which the Polycom DMA system logs into the SRC server.

**Table 7-5** Fields on the Juniper Networks SRC page (continued)

Field	Description
Client password	The password with which the Polycom DMA system logs into the SRC server.
Subscriber URI	The subscriber URI of an endpoint known to the SRC server, specified as in this example: <pre>ip:ipAddress=192.168.70.228</pre> This can be any endpoint about which the SRC server will return information when queried to test the connection.

See also:

[“Juniper Networks SRC Integration”](#) on page 161

[“Juniper Networks SRC Integration Procedure”](#) on page 162

## Juniper Networks SRC Integration Procedure

### To configure SRC integration

- 1 Go to **Admin > Integrations > Juniper Networks SRC**.
- 2 Check **Enable integration with Juniper Networks® SRC** and specify the address of the SRC server.
- 3 Specify the login credentials for the system to connect to the SRC server.
- 4 Specify the subscriber URI of an endpoint known to the SRC server, specified as in this example:

```
ip:ipAddress=192.168.70.228
```

This can be any endpoint about which the SRC server will return information when queried to test the connection.

- 5 Click **Update**.

To verify that it can successfully communicate with the SRC server, the Polycom DMA system queries the SRC server about the endpoint you specified and confirms that the query is successful. A dialog box informs you that the configuration has been updated.

- 6 Click **OK**.

See also:

[“Juniper Networks SRC Integration”](#) on page 161

[“Juniper Networks SRC Page”](#) on page 161

# Conference Manager Configuration

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system configuration topics related to the Conference Manager functionality:

- [Conference Settings](#)
- [Conference Templates](#)
- [Shared Number Dialing](#)

## Conference Settings

On the **Conference Settings** page, you can define the default class of service and bit rate limits, a dialing prefix, and various default conference properties for the Polycom DMA system. The table below describes them.

### Note

The default class of service, maximum bit rate, and minimum downspeed rate are the default values for point-to-point calls as well as conference (VMR) calls.

**Table 8-1** Fields on the Conference Settings page

Field	Description
Default class of service	The class of service assigned to a user or endpoint if the class of service isn't specified at the endpoint, user, or group level.
Default maximum bit rate (kbps)	The maximum bit rate for a call if the maximum bit rate for the user or endpoint isn't specified at the endpoint, user, or group level.
Default minimum downspeed (kbps)	The minimum bit rate to which a call can be reduced (downspeeded) if the minimum downspeed for the user or endpoint isn't specified at the endpoint, user, or group level.

**Table 8-1** Fields on the Conference Settings page (continued)

Field	Description
Dialing prefix	<p>E.164 dial string prefix for calling the system.</p> <p>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.</p> <p>If a prefix is specified, it's used for SIP calls as well so that the same number can be dialed from both H.323 and SIP endpoints.</p> <p><b>Caution:</b> Changing the dialing prefix terminates any existing H.323 calls. When you click <b>Update</b>, the system prompts you to confirm.</p>
Default max total participants	<p>Specifies the maximum conference size assigned to a conference room if a larger or smaller maximum size isn't specified for it.</p> <p><b>Automatic</b> (the default setting) uses the largest conference size supported by the MCU as the default maximum.</p>
Default conference template	<p>Default template used by the system. See <a href="#">"Conference Templates"</a> on page 165.</p>
Default territory	<p>The territory assigned to a user's conference room if it isn't specified at the user or conference room level.</p> <p>A conference room's territory assignment determines which 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.</p>
Default MCU pool order	<p>Default MCU pool order used by the system. See <a href="#">"MCU Pool Orders"</a> on page 130.</p>
Minimum and maximum generated room ID	<p>Specify the minimum and maximum values for auto-generated room IDs created for custom conference rooms. Values may be up to six digits long, and the minimum must be less than the maximum.</p> <p>The six-digit limit applies only to generated IDs for custom conference rooms.</p>
Conference Duration	<p>Default maximum duration of a conference (in hours and minutes) or <b>Unlimited</b> (the maximum in this case depends on the MCU).</p>

**To specify conference settings**

- 1 Go to **Admin > Conference Manager > Conference Settings**.
- 2 On the **Conference Settings** page, make the appropriate selections.



### 3 Click **Update**.

See also:

[“Conference Templates”](#) on page 165

[“Shared Number Dialing”](#) on page 190

## Conference Templates

Conference templates are used to create users’ 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.

### Note

This version of the Polycom DMA system supports the use of Cisco (formerly Tandberg) Codian 4200, 4500, and MSE 8000 series MCUs, and conference templates can include Codian-specific settings.

## Two Types of Templates

You can create a conference template in two ways:

- Specify the individual conference properties directly in the Polycom DMA system, creating a “standalone” template independent of the profiles available on the system’s RMX MCUs.
- Link the template to an RMX profile that exists on some or all of the MCUs.

Either kind of template can also include settings specific to Cisco Codian MCUs so that it can be used in deployments containing both kinds of MCUs.

### Standalone Templates

Standalone templates defined in the Polycom DMA system free you from having to ensure that the exact same RMX profiles exist on all the MCUs. You specify the desired conference properties directly in the template.

When it uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of its profiles.

When using a template not linked to an RMX profile, the system doesn’t use the template’s properties to limit its choice of MCU. It selects the least used MCU in the selected MCU pool (see [“MCU Pools”](#) on page 127 and [“MCU Pool Orders”](#) on page 130). 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, that property is ignored.

To preferentially route conferences to certain MCUs, use MCU pool orders. See [“MCU Pools”](#) on page 127 and [“MCU Pool Orders”](#) on page 130.

## Templates Linked to RMX Profiles

Linking a template to an RMX profile lets you access profile properties that aren't currently available in a standalone template.

### Note

You can also use a template linked to an RMX profile to preferentially route conferences to RMX MCUs that have the profile. But we recommend that you create MCU pools and pool orders for this purpose instead of using profiles. See [“MCU Pools”](#) on page 127 and [“MCU Pool Orders”](#) on page 130.

When you link a template to a profile, it's up to you to ensure that the profile exists on the MCUs you want to use with that template and that its settings are the same on all of them.

When it uses a profile-based template, the system first tries to find an MCU that has that profile (but it does so within the MCU pool order rules; see [“MCU Pools”](#) on page 127 and [“MCU Pool Orders”](#) on page 130). It 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 RMX MCU, it falls back to its default conference template (see [“Conference Settings”](#) on page 163). 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.

See also:

[“Conference Templates”](#) on page 165

[“Template Priority”](#) on page 167

[“About Conference IVR Services”](#) on page 167

[“About Cascading”](#) on page 168

[“Conference Templates Procedures”](#) on page 188

## Template Priority

A user (local or enterprise) has one or more conference rooms. Each room may either use the system's default template (specified on the [Conference Settings](#) page) or use a specifically assigned template. (Typically, 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 these rules (in order of importance) to determine which template to use for the conference:

- 1 If the conference room has a specifically assigned template (not the system default) associated with it, 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.

See also:

["Conference Templates"](#) on page 165

["Two Types of Templates"](#) on page 165

["About Conference IVR Services"](#) on page 167

["About Cascading"](#) on page 168

["Conference Templates Procedures"](#) on page 188

## About Conference IVR Services

One of the conference properties you can optionally specify in a template is the conference IVR service that the RMX MCU should use. For most purposes, you shouldn't do so. RMX MCUs have two defaults, one for conferences with passcodes and one for conferences without passcodes, and automatically use the right one for each conference.

If you do choose to override the default and specify an IVR service, it's up to you to make sure that the IVR service you select is appropriate for the users whose conferences will use this template, and that it's available on the MCUs on which those conference may take place. See your Polycom RMX documentation for information about conference IVR services. This feature is not supported on Cisco (formerly Tandberg) Codian MCUs.

On the **Conference IVR** tab of the **Add Conference Template** and **Edit Conference Template** dialog boxes, 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 instance, 2 of 3).

If a template specifies a conference IVR service, the system will put conferences using that template on the least used RMX MCU that has that conference IVR service. If there are none, it falls back to the default conference IVR service.

See also:

[“Conference Templates”](#) on page 165

[“Two Types of Templates”](#) on page 165

[“Template Priority”](#) on page 167

[“About Cascading”](#) on page 168

[“Conference Templates Procedures”](#) on page 188

## About Cascading

One of the conference features you can optionally enable in a template is cascading, which makes it possible for a conference to span RMX MCUs. Cascading a conference across multiple MCUs can conserve bandwidth and 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.

Cascading does, however, impact the quality of the conference experience.

### Note

The cascade links between RMX MCUs must use H.323 signaling. For conferences with cascading enabled, the Polycom 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 Polycom DMA system are also configured for SIP signaling).

If you have a Polycom CMA system in your network, you can enable cascaded conferences with these steps:

- 1 On the Polycom CMA system, create site topology data defining the territories, sites, site links, and MPLS clouds in your network, and the subnets in each site.
- 2 On the Polycom DMA system, integrate with the Polycom CMA system to obtain its site topology data. See [“Polycom CMA System Integration”](#) on page 157.

- 3 On the Polycom DMA system, enable cascading in some or all of your conference templates.

If you don't have a Polycom CMA system, you must define your site topology in the Polycom DMA system instead of importing it. See ["Site Topology"](#) on page 241.

#### Note

Cascading always uses a hub-and-spoke configuration so that each cascaded MCU is only one link away from the "hub" MCU, which hosts the conference. To host the conference, the system chooses the same MCU that it would have chosen in the absence of cascading. See ["MCU Pool Orders"](#) on page 130.

Once a conference with cascading enabled has started (the "hub" MCU has been chosen), the Polycom DMA system uses the site topology information to route additional callers to the nearest eligible MCU (based on pools and pool orders) that has available capacity. If that MCU is new to the conference, the DMA system creates the cascade link to the "hub" MCU hosting the conference.

See also:

["Conference Templates"](#) on page 165

["Two Types of Templates"](#) on page 165

["Template Priority"](#) on page 167

["About Conference IVR Services"](#) on page 167

["Conference Templates Procedures"](#) on page 188

## Conference Templates List

The following table describes the fields in the **Conference Templates** list.

**Table 8-2** Information in the Conference Templates list

Column	Description
Priority	The priority ranking of the template.
Name	The name of the template.
Description	A description of the template.

The Polycom DMA system comes with a **Factory Template** that has a default set of conference parameters. You can edit it and create additional templates.

See also:

["Conference Templates"](#) on page 165

["Add Conference Template Dialog Box"](#) on page 170

[“Edit Conference Template Dialog Box”](#) on page 179

[“Conference Templates Procedures”](#) on page 188

## Add Conference Template Dialog Box

Lets you add a conference template. The following table describes the fields in the dialog box. The **Common Settings** section applies to all MCUs. The **Tandberg Codian** section appears only if the system is licensed to use Cisco (formerly Tandberg) Codian MCUs, and its settings apply only if a Codian MCU is selected for the call. The other sections apply only if an RMX MCU is selected.

**Table 8-3** Add Conference Template dialog box

Field	Description
<b>Common Settings</b>	
Name	A meaningful name for the template (up to 50 characters).
Description	A brief description of the conference template (up to 50 characters).
<b>RMX General Settings</b>	
Use existing profile	Links this template to the RMX profile selected in the list below.  For most purposes, we recommend leaving this box unchecked and specifying conference properties directly. See <a href="#">“Conference Templates”</a> on page 165.
RMX profile name	Identifies the RMX 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 (for instance, 2 of 3).  The system will put conferences using this template on the least used RMX MCU that has this profile. If there are none, it selects the least-used MCU and either uses the Codian-specific settings (if it selected a Codian MCU) or falls back to the default conference template (if it selected a Polycom RMX MCU).

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
Cascaded conference	<p>Enables conferences using this template to span RMX MCUs.</p> <p>Cascading requires site topology information, which the Polycom DMA system can get from a Polycom CMA system (see <a href="#">“Polycom CMA System Integration”</a> on page 157) or you can create (see <a href="#">“Site Topology”</a> on page 241).</p> <p>See <a href="#">“About Cascading”</a> on page 168 for more information about enabling cascading of conferences.</p>
Video switching (VSW)	<p>Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker).</p> <p>If this mode is enabled:</p> <ul style="list-style-type: none"> <li>• The minimum line rate available is 768 kbps (except for SD resolution, available only on RMX v7 MCUs with MPM+ or MPMx cards).</li> <li>• 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.</li> <li>• The video clarity, layout, and skins settings are not available.</li> <li>• LPR is automatically turned off, but can be turned back on.</li> </ul> <p>If this option is off, conferences using this template are in Continuous Presence (CP) mode, in which the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities.</p>
H.264 high profile	<p>Sets a VSW conference to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode).</p> <p>If this is selected, all endpoints in the conference must support High Profile. Endpoints not connecting at the conference's exact line rate and resolution are connected in audio-only mode. Available only on RMX v7.6 or later MCUs with MPMx cards.</p>

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
Resolution	<p>Available only if <b>Video switching</b> is selected. Offers four resolution settings:</p> <ul style="list-style-type: none"> <li>• H.264 720p30</li> <li>• H.264 1080p30 (available only on RMX MCUs with MPM+ or MPMx cards)</li> <li>• H.264 SD 30 (available only on RMX v7 MCUs with MPM+ or MPMx cards)</li> <li>• H.264 720p60 (available only on RMX v7 MCUs with MPM+ or MPMx cards)</li> <li>• H.264 CIF (available only on RMX v7 MCUs)</li> <li>• H.263 CIF (available only on RMX v7 MCUs)</li> <li>• H.261 CIF (available only on RMX v7 MCUs)</li> </ul>
Line rate	<p>The maximum bit rate at which endpoints can connect to conferences using this template.</p> <p>If <b>Video switching</b> is selected, the lowest line rate available is 768 kbps (except for SD resolution, available only on RMX v7 MCUs with MPM+ or MPMx cards).</p>
Encryption	<p>Specifies that media encryption should be required for conferences using this template.</p> <p>In general, enabling this option prevents unencrypted endpoints from joining a conference. But the effect of this setting depends on the RMX MCU's licensing and other configuration settings. Consult the <i>Polycom RMX 1500/2000/4000 Administrator's Guide</i> for detailed information about media encryption.</p>
LPR	<p>Enables <i>Lost Packet Recovery</i> for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission.</p>
TIP compatibility	<p>Enables compatibility with Cisco's Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences can include both endpoints that don't support TIP and Cisco TelePresence® System (CTS) endpoints.</p> <p>Requires minimum line rate of 1024 kbps and HD resolution (720 or better). Available only on RMX v7.6 or later MCUs.</p>



**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
<b>RMX Gathering Settings</b>	
Enable gathering	Enables the gathering phase feature for conferences using this template. Available only on RMX v. 6.0 or later MCUs. The gathering phase is a time period (configurable on the RMX MCU) at the beginning of a conference, when people are connecting. During this time, a slide is displayed that contains conference information, including a list participants and some information you can specify here.
Displayed language	Language in which the gathering page is displayed.
Access number 1	Optional access numbers to display on the gathering phase slide.
Access number 2	
Info1	Optional free-form text fields to display on the gathering phase slide. Refer to the <i>RMX Administrator's Guide</i> 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.
Info2	
Info3	
<b>RMX Video Quality</b>	
Video quality	Offers two video optimizations: <ul style="list-style-type: none"> <li>• Motion — higher frame rate</li> <li>• Sharpness — higher resolution</li> </ul>
Max resolution	The four resolution settings limit the conference to no more than that resolution regardless of the line rate and resolution capabilities of the MCU and endpoints. Auto (the default) imposes no limit. Available only on RMX v7 MCUs.
Video clarity	Enables a video enhancement process that improves clarity, edge sharpness, and contrast on streams with resolutions up to and including SD. Available only on RMX MCUs with MPM+ or MPMx cards. Not available if <b>Video switching</b> is selected.
Auto brightness	Enables automatic balancing of brightness levels to compensate for an endpoint sending a dim image. Available only on RMX v7 MCUs.

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
Content settings	<p>The transmission mode for the Content channel:</p> <ul style="list-style-type: none"> <li>Graphics — lowest bit rate for basic graphics</li> <li>High-resolution graphics — higher bit rate for better graphics resolution</li> <li>Live video — the Content channel is used for live video</li> </ul> <p>A higher bit rate for the Content channel reduces the bit rate for the People channel.</p>
Content protocol	<p>Content channel protocol options:</p> <ul style="list-style-type: none"> <li>Use H.264 if available, otherwise use H.263.</li> <li>Always use H.263.</li> </ul>
<b>RMX Video Settings</b>	
Presentation mode	<p>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.</p> <p>Not available if <b>Video switching</b> or <b>Same layout</b> is selected, or if <b>Telepresence mode</b> is Yes.</p>
Send content to legacy endpoints	<p>Enables endpoints that don't support H.239 to receive the Content channel over the video (People) channel.</p> <p>Available only on MCUs with MPM+ and MPMx cards. Not available if <b>Video switching</b> or <b>Same layout</b> is selected, or if <b>Telepresence mode</b> is Yes.</p>
Same layout	<p>Forces the selected layout on all participants. Personal selection of the video layout is disabled.</p> <p>Not available if <b>Presentation mode</b> or <b>Video switching</b> is selected, or if <b>Telepresence mode</b> is Yes.</p>
Lecturer view switching	<p>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.</p> <p>Not available if <b>Same layout</b> is selected or <b>Telepresence mode</b> is Yes.</p>
Auto layout	<p>Lets the system select the video layout based on the number of participants in conference. Clear the check box to select a specific layout (below).</p> <p>Not available if <b>Video switching</b> is selected or <b>Telepresence mode</b> is Yes.</p>

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
Layout	<p>With <b>Auto layout</b> deselected, this opens the <b>Select Layout</b> dialog box, where you can select the number and arrangement of video frames. Once a layout is chosen, a small representation of it appears here. See <a href="#">“Select Layout Dialog Box”</a> on page 187.</p> <p>Not available if <b>Video switching</b> is selected.</p>
Telepresence mode	<p>Support for telepresence conference rooms joining the conference:</p> <ul style="list-style-type: none"> <li>• Auto (default) — A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins.</li> <li>• Yes — Telepresence mode is on, regardless of whether a telepresence endpoint is present.</li> <li>• No — Telepresence mode is off, regardless of whether a telepresence endpoint is present.</li> </ul> <p>Available only on RMX v. 6.0 or later MCUs that are licensed for telepresence mode. We recommend always using Auto.</p> <p><b>Note:</b> The RMX system flag ITP_CERTIFICATION must be set to YES. See Table 19-3, “Manually Added System Flags — MCMS_PARAMETERS” in the <i>Polycom RMX Administrator’s Guide</i>.</p>
Telepresence layout mode	<p>Layout choices for telepresence conferences:</p> <ul style="list-style-type: none"> <li>• Manual — Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface.</li> <li>• Continuous Presence — Tells the MLA to generate a multipoint view (standard or custom).</li> <li>• Room Switch — Tells the MLA to use Voice Activated Room Switching (VARS). The speaker’s site is the only one seen by others.</li> </ul> <p>Not available if <b>Telepresence mode</b> is No. See the <i>Polycom Multipoint Layout Application User Guide</i> for more information about layouts.</p>
<b>RMX Audio Settings</b>	
Echo suppression	<p>Enables the MCU to detect and suppress echo.</p> <p>Available only on MCUs with MPM+ or MPMx cards.</p>
Keyboard suppression	<p>Enables the MCU to detect and suppress keyboard noise.</p> <p>Available only on MCUs with MPM+ or MPMx cards.</p>
Audio clarity	<p>Improves the voice quality in conference of a PSTN endpoint.</p> <p>Available only on RMX v7 MCUs.</p>

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
<b>RMX Skins</b>	Lets you choose the display appearance (skin) for conferences using this template.  Not available if <b>Telepresence mode</b> is Yes. or <b>Video switching</b> is enabled.
<b>RMX Conference IVR</b>	
Override default conference IVR service	Links this template to the specific conference IVR service selected in the list below.  For most purposes, this option should not be selected. That 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. See your Polycom RMX documentation for information about conference IVR services.
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 instance, 2 of 3).  The system will put conferences using this template on the least used RMX MCU that has the selected conference IVR service. If there are none, it falls back to the default conference IVR service.
Conference requires chairperson	Conferences based on this template don't start until a chairperson joins (callers arriving earlier are placed on hold) and 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. See <a href="#">"Adding Passcodes for Enterprise Users"</a> on page 146. But you can override the Active Directory value; see <a href="#">"Edit User Dialog Box"</a> on page 272.  For local users, you can add or change chairperson passcodes when you create or edit the users. See <a href="#">"Edit User Dialog Box"</a> on page 272.

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
<b>RMX Recording</b>	
Record conference	<p>The conference recording setting for this template:</p> <ul style="list-style-type: none"> <li>• Disabled — Recording isn't available for conferences using this template.</li> <li>• Immediately — Recording starts automatically when the conference starts.</li> <li>• Upon Request — Recording can be initiated manually by the chairperson or an operator.</li> </ul> <p>Conference recording requires a Polycom RSS recording system and an MCU that supports recording.</p>
Recording link	<p>Select a specific recording link or the MCU's default. 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. Available only on RMX v7 MCUs.</p>
Audio only	Limits recording to the audio channel of the conference.
Indication of recording	<p>Displays a red dot recording indicator in the upper left corner of the video layout. Available only on RMX v7.1 MCUs.</p>
<b>Tandberg Codian</b>	
Floor and chair control	<p>Specifies how much control conference participants may have:</p> <ul style="list-style-type: none"> <li>• Do not allow — Participants have no control.</li> <li>• Floor only — A participant may "take the floor." Everyone sees that participant's video full-screen.</li> <li>• Floor and chair control — A participant may also "take the chair." The chair can designate whose video everyone sees full-screen. The chair can also disconnect participants.</li> </ul> <p>This setting works only in H.323 conferences and only if H.243 Floor and Chair Control is enabled on the MCU. All endpoints must support H.243 chair control.</p>
Automatic lecture mode	<p>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. Available only on Codian v4.1 MCUs.</p>

**Table 8-3** Add Conference Template dialog box (continued)

Field	Description
Layout control via FECC/DTMF	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. FECC without fallback is available only on Codian v4.1 MCUs.
Mute in-band DTMF	Specifies whether the MCU mutes participants' in-band DTMF (touchtones) so that other participants don't hear them: <ul style="list-style-type: none"> <li>• When used for MCU control</li> <li>• Always</li> <li>• Never</li> </ul> Available only on Codian v4.1 MCUs.
Allow DTMF *6 to mute audio	Enables conference participants to mute themselves using the *6 touchtone command. Available only on Codian v4.1 MCUs.
Content channel video	Enables the conference to support a second video stream for content. This setting works only if Content Status is enabled on the MCU.
Transmitted content resolutions	Specifies the aspect ratio used for the content channel. If <b>Allow all resolutions</b> is selected, endpoints with a 16:9 aspect ratio receive that, and others receive 4:3. Available only on Codian v4.1 MCUs.
Conference custom layout	Opens the <b>Select Layout</b> dialog box, where you can select the number and arrangement of video frames. Once a layout is chosen, a small representation of it appears here. See " <a href="#">Select Layout Dialog Box</a> " on page 187.

See also:

["Conference Templates"](#) on page 165

["Edit Conference Template Dialog Box"](#) on page 179

["Select Layout Dialog Box"](#) on page 187

["Conference Templates Procedures"](#) on page 188

## Edit Conference Template Dialog Box

Lets you edit a conference template. The following table describes the fields in the dialog box. The **Common Settings** section applies to all MCUs. The **Tandberg Codian** section appears only if the system is licensed to use Cisco (formerly Tandberg) Codian MCUs, and its settings apply only if a Codian MCU is selected for the call. The other sections apply only if an RMX MCU is selected.

**Table 8-4** Edit Conference Template dialog box

Field	Description
<b>Common Settings</b>	
Name	A meaningful name for the template (up to 50 characters).
Description	A brief description of the conference template (up to 50 characters).
<b>RMX General Settings</b>	
Use existing profile	Links this template to the RMX profile selected in the list below.  For most purposes, we recommend leaving this box unchecked and specifying conference properties directly. See <a href="#">“Conference Templates”</a> on page 165.
RMX profile name	Identifies the RMX 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 (for instance, 2 of 3).  The system will put conferences using this template on the least used RMX MCU that has this profile. If there are none, it selects the least-used MCU and either uses the Codian-specific settings (if it selected a Codian MCU) or falls back to the default conference template (if it selected a Polycom RMX MCU).
Cascaded conference	Enables conferences using this template to span RMX MCUs.  Cascading requires site topology information, which the Polycom DMA system can get from a Polycom CMA system (see <a href="#">“Polycom CMA System Integration”</a> on page 157) or you can create (see <a href="#">“Site Topology”</a> on page 241).  See <a href="#">“About Cascading”</a> on page 168 for more information about enabling cascading of conferences.

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Video switching (VSW)	<p>Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker).</p> <p>If this mode is enabled:</p> <ul style="list-style-type: none"> <li>• The minimum line rate available is 768 kbps (except for SD resolution, available only on RMX v7 MCUs with MPM+ or MPMx cards).</li> <li>• 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.</li> <li>• The video clarity, layout, and skins settings are not available.</li> <li>• LPR is automatically turned off, but can be turned back on.</li> </ul> <p>If this option is off, conferences using this template are in Continuous Presence (CP) mode, in which the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities.</p>
H.264 high profile	<p>Sets a VSW conference to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode).</p> <p>If this is selected, all endpoints in the conference must support High Profile. Endpoints not connecting at the conference's exact line rate and resolution are connected in audio-only mode. Available only on RMX v7.6 or later MCUs with MPMx cards.</p>
Resolution	<p>Available only if <b>Video switching</b> is selected. Offers the following resolution settings:</p> <ul style="list-style-type: none"> <li>• H.264 720p30</li> <li>• H.264 1080p30 (available only on RMX MCUs with MPM+ or MPMx cards)</li> <li>• H.264 SD 30 (available only on RMX v7 MCUs with MPM+ or MPMx cards)</li> <li>• H.261 CIF (available only on RMX v7 MCUs)</li> <li>• H.263 CIF (available only on RMX v7 MCUs)</li> <li>• H.264 CIF (available only on RMX v7 MCUs)</li> <li>• H.264 720p60 (available only on RMX v7 MCUs with MPM+ or MPMx cards)</li> </ul>
Line rate	<p>The maximum bit rate at which endpoints can connect to conferences using this template.</p> <p>If <b>Video switching</b> is selected, the lowest line rate available depends on the <b>Resolution</b> setting chosen.</p>



**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Encryption	Specifies that media encryption should be required for conferences using this template.  In general, enabling this option prevents unencrypted endpoints from joining a conference. But the effect of this setting depends on the RMX MCU's licensing and other configuration settings. Consult the <i>Polycom RMX 1500/2000/4000 Administrator's Guide</i> for detailed information about media encryption.
LPR	Enables <i>Lost Packet Recovery</i> for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission.
TIP compatibility	Enables compatibility with Cisco's Telepresence Interoperability Protocol, either for video only or for both video and content. Conferences can include both endpoints that don't support TIP and Cisco TelePresence® System (CTS) endpoints.  Requires minimum line rate of 1024 kbps and HD resolution (720 or better). Available only on RMX v7.6 or later MCUs.
<b>RMX Gathering Settings</b>	
Enable gathering	Enables the Gathering Phase feature for conferences using this template.  Available only on RMX v. 6.0 or later MCUs.  The Gathering Phase is a time period (configurable on the RMX MCU) at the beginning of a conference, when people are connecting. During this time, a slide is displayed that contains conference information, including a list participants and some information you can specify here.
Displayed language	Language in which the gathering page is displayed.
Access number 1	Optional access numbers to display on the Gathering Phase slide.
Access number 2	
Info1	Optional free-form text fields to display on the Gathering Phase slide. Refer to the <i>RMX Administrator's Guide</i> 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.
Info2	
Info3	

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
<b>RMX Video Quality</b>	
Video quality	Offers two video optimizations: <ul style="list-style-type: none"> <li>• Motion — higher frame rate</li> <li>• Sharpness — higher resolution</li> </ul>
Max resolution	The four resolution settings limit the conference to no more than that resolution regardless of the line rate and resolution capabilities of the MCU and endpoints. Auto (the default) imposes no limit. Available only on RMX v7 MCUs.
Video clarity	Enables a video enhancement process that improves clarity, edge sharpness, and contrast on streams with resolutions up to and including SD. Available only on RMX MCUs with MPM+ or MPMx cards. Not available if <b>Video switching</b> is selected.
Auto brightness	Enables automatic balancing of brightness levels to compensate for an endpoint sending a dim image. Available only on RMX v7 MCUs.
Content settings	The transmission mode for the Content channel: <ul style="list-style-type: none"> <li>• Graphics — lowest bit rate for basic graphics</li> <li>• High-resolution graphics — higher bit rate for better graphics resolution</li> <li>• Live video — the Content channel is used for live video</li> </ul> A higher bit rate for the Content channel reduces the bit rate for the People channel.
Content protocol	Content channel protocol options: <ul style="list-style-type: none"> <li>• Use H.264 if available, otherwise use H.263.</li> <li>• Always use H.263.</li> </ul>
<b>RMX Video Settings</b>	
Presentation mode	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. Not available if <b>Video switching</b> or <b>Same layout</b> is selected, or if <b>Telepresence mode</b> is Yes.
Send content to legacy endpoints	Enables endpoints that don't support H.239 to receive the Content channel over the video (People) channel. Available only on MCUs with MPM+ and MPMx cards. Not available if <b>Video switching</b> or <b>Same layout</b> is selected, or if <b>Telepresence mode</b> is Yes.

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Same layout	Forces the selected layout on all participants. Personal selection of the video layout is disabled. Not available if <b>Presentation mode</b> or <b>Video switching</b> is selected, or if <b>Telepresence mode</b> is Yes.
Lecturer view switching	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. Not available if <b>Same layout</b> is selected or <b>Telepresence mode</b> is Yes.
Auto layout	Lets the system select the video layout based on the number of participants in conference. Clear the check box to select a specific layout (below). Not available if <b>Video switching</b> is on or <b>Telepresence mode</b> is Yes.
Layout	With <b>Auto layout</b> deselected, this opens the <b>Select Layout</b> dialog box, where you can select the number and arrangement of video frames. Once a layout is chosen, a small representation of it appears here. See <a href="#">"Select Layout Dialog Box"</a> on page 187. Not available if <b>Video switching</b> is on.
Telepresence mode	Support for telepresence conference rooms joining the conference: <ul style="list-style-type: none"> <li>• Auto (default) — A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins.</li> <li>• Yes — Telepresence mode is on, regardless of whether a telepresence endpoint is present.</li> <li>• No — Telepresence mode is off, regardless of whether a telepresence endpoint is present.</li> </ul> Available only on RMX v. 6.0 or later MCUs that are licensed for telepresence mode. We recommend always using Auto. <b>Note:</b> The RMX system flag ITP_CERTIFICATION must be set to YES. See Table 19-3, "Manually Added System Flags — MCMS_PARAMETERS" in the <i>Polycom RMX Administrator's Guide</i> .

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Telepresence layout mode	<p>Layout choices for telepresence conferences:</p> <ul style="list-style-type: none"> <li>• Manual — Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface.</li> <li>• Continuous Presence — Tells the MLA to generate a multipoint view (standard or custom).</li> <li>• Room Switch — Tells the MLA to use Voice Activated Room Switching (VARs). The speaker's site is the only one seen by others.</li> </ul> <p>Not available if <b>Telepresence mode</b> is No. See the <i>Polycom Multipoint Layout Application User Guide</i> for more information about layouts.</p>
<b>RMX Audio Settings</b>	
Echo suppression	<p>Enables the MCU to detect and suppress echo. Available only on MCUs with MPM+ or MPMx cards.</p>
Keyboard suppression	<p>Enables the MCU to detect and suppress keyboard noise. Available only on MCUs with MPM+ or MPMx cards.</p>
Audio clarity	<p>Improves the voice quality in conference of a PSTN endpoint. Available only on RMX v7 MCUs.</p>
<b>RMX Skins</b>	<p>Lets you choose the display appearance (skin) for conferences using this template. Not available if <b>Telepresence mode</b> is Yes. or <b>Video switching</b> is enabled.</p>
<b>RMX Conference IVR</b>	
Override default conference IVR service	<p>Links this template to the specific conference IVR service selected in the list below. For most purposes, this option should not be selected. That 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. See your Polycom RMX documentation for information about conference IVR services.</p>

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Conference IVR service	<p>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 instance, 2 of 3).</p> <p>The system will put conferences using this template on the least used RMX MCU that has the selected conference IVR service. If there are none, it falls back to the default conference IVR service.</p>
Conference requires chairperson	<p>Conferences based on this template don't start until a chairperson joins (callers arriving earlier are placed on hold) and may end when the last chairperson leaves (depending on the MCU configuration).</p> <p>This option is ignored if the user doesn't have a chairperson passcode.</p> <p>For enterprise users, chairperson passcodes can come from the Active Directory. See <a href="#">"Adding Passcodes for Enterprise Users"</a> on page 146. But you can override the Active Directory value; see <a href="#">"Edit User Dialog Box"</a> on page 272.</p> <p>For local users, you can add or change chairperson passcodes when you create or edit the users. See <a href="#">"Edit User Dialog Box"</a> on page 272.</p>
<b>RMX Recording</b>	
Record conference	<p>The conference recording setting for this template:</p> <ul style="list-style-type: none"> <li>• Disabled — Recording isn't available for conferences using this template.</li> <li>• Immediately — Recording starts automatically when the conference starts.</li> <li>• Upon Request — Recording can be initiated manually by the chairperson or an operator.</li> </ul> <p>Conference recording requires a Polycom RSS recording system and an MCU that supports recording.</p>
Recording link	<p>Select a specific recording link or the MCU's default. 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.</p> <p>Available only on RMX v7 MCUs.</p>
Audio only	Limits recording to the audio channel of the conference.
Indication of recording	<p>Displays a red dot recording indicator in the upper left corner of the video layout.</p> <p>Available only on RMX v7.1 MCUs.</p>

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
<b>Tandberg Codian</b>	
Floor and chair control	<p>Specifies how much control conference participants may have:</p> <ul style="list-style-type: none"> <li>Do not allow — Participants have no control.</li> <li>Floor only — A participant may “take the floor.” Everyone sees that participant’s video full-screen.</li> <li>Floor and chair control — A participant may also “take the chair.” The chair can designate whose video everyone sees full-screen. The chair can also disconnect participants.</li> </ul> <p>This setting works only in H.323 conferences and only if H.243 Floor and Chair Control is enabled on the MCU. All endpoints must support H.243 chair control.</p>
Automatic lecture mode	<p>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.</p> <p>Available only on Codian v4.1 MCUs.</p>
Layout control via FECC/DTMF	<p>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.</p> <p>FECC without fallback is available only on Codian v4.1 MCUs.</p>
Mute in-band DTMF	<p>Specifies whether the MCU mutes participants’ in-band DTMF (touchtones) so that other participants don’t hear them:</p> <ul style="list-style-type: none"> <li>When used for MCU control</li> <li>Always</li> <li>Never</li> </ul> <p>Available only on Codian v4.1 MCUs.</p>
Allow DTMF *6 to mute audio	<p>Enables conference participants to mute themselves using the *6 touchtone command.</p> <p>Available only on Codian v4.1 MCUs.</p>

**Table 8-4** Edit Conference Template dialog box (continued)

Field	Description
Content channel video	Enables the conference to support a second video stream for content.  This setting works only if Content Status is enabled on the MCU.
Transmitted content resolutions	Specifies the aspect ratio used for the content channel. If <b>Allow all resolutions</b> is selected, endpoints with a 16:9 aspect ratio receive that, and others receive 4:3. Available only on Codian v4.1 MCUs.
Conference custom layout	Opens the <b>Select Layout</b> dialog box, where you can select the number and arrangement of video frames. Once a layout is chosen, a small representation of it appears here. See <a href="#">“Select Layout Dialog Box”</a> on page 187.

See also:

[“Conference Templates”](#) on page 165

[“Add Conference Template Dialog Box”](#) on page 170

[“Select Layout Dialog Box”](#) on page 187

[“Conference Templates Procedures”](#) on page 188

## Select Layout Dialog Box

Lets you select a specific video frames layout when you’re adding or editing a conference template.

### To select a video frames layout

- 1 For a Polycom RMX MCU, choose a **Frame count value** to see the layouts available for that value, and then select the one you want.
- 2 For a Cisco (formerly Tandberg) Codian MCU, select the layout you want.
- 3 Click **OK**.

See also:

[“Conference Templates”](#) on page 165

[“Add Conference Template Dialog Box”](#) on page 170

[“Edit Conference Template Dialog Box”](#) on page 179

[“Conference Templates Procedures”](#) on page 188

## Conference Templates Procedures

### To view the Conference Templates list

>> Go to **Admin > Conference Manager > Conference Templates**.

The **Conference Templates** list appears.

### To add a conference template not linked to an RMX profile

- 1 Go to **Admin > Conference Manager > Conference Templates**.
- 2 In the **Actions** list, click **Add**.
- 3 In the **Add Conference Template** dialog box, specify all the conference properties for this template:
  - a In **Common Settings**, enter an appropriate name and description.
  - b To enable conferences using this template to cascade across multiple MCUs, check **Cascaded conference** in **RMX General Settings**.
  - c Complete the remaining sections as desired. See [“Add Conference Template Dialog Box”](#) on page 170.
- 4 Click **OK**.

The new template appears in the **Conference Templates** list.

### To add a conference template linked to an RMX profile

- 1 Go to **Admin > Conference Manager > Conference Templates**.
- 2 In the **Actions** list, click **Add**.
- 3 In the **Add Conference Template** dialog box, specify all the conference properties for this template:
  - a In **Common Settings**, enter an appropriate name and description.
  - b To enable conferences using this template to cascade across multiple MCUs, check **Cascaded conference** in **RMX General Settings**.
  - c Check **Use existing profile** and select the one you want from the **RMX profile name** list.

The list contains the profiles available on the RMX MCUs that have been added to the Polycom DMA system.

- 4 Click **OK**.

The new template appears in the **Conference Templates** list.



**To edit a conference template**

- 1 Go to **Admin > Conference Manager > Conference Templates**.
- 2 In the **Conference Templates** list, select the template of interest, and in the **Actions** list, click **Edit**.
- 3 In the **Edit Conference Template** dialog box, edit the settings as desired. See [“Edit Conference Template Dialog Box”](#) on page 179.
- 4 Click **OK**.

The template changes appear in the **Conference Templates** list.

**To change a conference template’s priority**

- 1 Go to **Admin > Conference Manager > 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. We recommend moving the system default template to the bottom of the list.

- 4 Repeat until the template has the desired ranking.

**To delete a conference template**

- 1 Go to **Admin > Conference Manager > Conference Templates**.
- 2 In the **Conference Templates** list, select the template you want to delete, and in the **Actions** list, click **Delete**.
- 3 When asked to confirm that you want to delete the selected template, click **Yes**.

Any conference rooms or enterprise groups that used the template are reset to use the system default template.

See also:

[“Conference Templates”](#) on page 165

[“Add Conference Template Dialog Box”](#) on page 170

[“Edit Conference Template Dialog Box”](#) on page 179

## Shared Number Dialing

The shared number dialing feature enables you to publicize a shared number that can be used to reach multiple conferences, or virtual meeting rooms (VMRs). After callers dial the shared number, they're prompted for the VMR number to which they want to connect.

This feature is analogous to the behavior of entry queues on the Polycom RMX MCU, extending it to the DMA environment where the conference can start on any of the connected MCUs. The call flow works as follows:

- 1 Callers dial a shared number to reach the Polycom DMA system.
- 2 The Polycom DMA system recognizes the dialed number as a virtual entry queue (VEQ) number and routes the call to a Polycom RMX MCU configured to provide the entry queue interactive voice response (IVR) experience associated with the VEQ number dialed.
- 3 The MCU prompts the caller for the VMR number of the destination conference and sends the response back to the Polycom DMA system.
- 4 The Polycom DMA system validates the VMR number entered by the caller. If it's valid, the system routes the call to an appropriate MCU for the conference.

If the caller entered an invalid number, the system re-prompts the caller. The number of retries is configurable.

Shared number dialing requires SIP signaling and is supported only by v7.0.2 or later Polycom RMX MCUs. The default dial plan contains 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 instance, different language prompts or different greetings). You can designate one of the VEQs as the *Direct Dial VEQ*, and the system will use it for calls dialed without a VEQ or VMR number. For instance, if a call's dial string includes only the system's domain name or IP address, the Polycom DMA system uses the Direct Dial VEQ for it.

For each unique VEQ experience, you must create the corresponding RMX entry queue on the MCUs to be used for IVR prompting in this call flow.

### Note

The entry queues created for shared number dialing must have the **IVR service provider only** setting selected. See your Polycom RMX documentation.

When selecting an MCU to handle IVR for a VEQ, the Polycom DMA system chooses from among those that have the RMX entry queue specified for that VEQ, without regard to MCU pool orders.

As with conference profiles, it's up to you to ensure that the RMX entry queue is available on the MCUs to be used and that it's the same on each MCU.

The **Shared Number Dialing** page lists the VEQs available on the system and enables you to add, edit and delete VEQs. The following table describes the fields on the page.

**Table 8-5** *Fields on the Shared Number Dialing page*

Field	Description
Virtual Entry Queue	The VEQ number, such as <i>12345</i> , or <i>Direct Dial</i> .
Dial-In #	The complete dial string, for this VEQ. For instance, if the system uses the prefix <i>71</i> , this might be <i>7112345</i> .
Description	Typically, a description of the IVR experience, such as which language is used.
VMR Entry Attempts	The number of times a caller can enter an invalid VMR number before the system rejects the call.
RMX Entry Queue	The name of the RMX entry queue (IVR experience) to be used for callers to this VEQ.

See also:

[“Add Virtual Entry Queue Dialog Box”](#) on page 191

[“Add Direct Dial Virtual Entry Queue Dialog Box”](#) on page 192

[“Edit Virtual Entry Queue Dialog Box”](#) on page 193

[“Edit Direct Dial Virtual Entry Queue Dialog Box”](#) on page 193

[“Conference Templates”](#) on page 165

[“Conference Settings”](#) on page 163

## Add Virtual Entry Queue Dialog Box

Lets you add a virtual entry queue (VEQ) to the list of configured VEQs on the **Shared Number Dialing** page. The table below describes the fields in the dialog box.

**Table 8-6** *The fields in the Add Virtual Entry Queue dialog box*

Field	Description
Virtual entry queue	The VEQ number.
Description	A meaningful description for this VEQ and its IVR experience, such as which language is used.

**Table 8-6** The fields in the Add Virtual Entry Queue dialog box (continued)

Field	Description
VMR entry attempts	The number of times a caller can enter an invalid VMR number before the system rejects the call.
RMX entry queue	The RMX entry queue to use for this VEQ. The drop-down list includes all the RMX entry queues available on the MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.

See also:

[“Shared Number Dialing”](#) on page 190

## Add Direct Dial Virtual Entry Queue Dialog Box

Lets you add a direct dial virtual entry queue (VEQ) to the list of configured VEQs on the **Shared Number Dialing** page. The table below describes the fields in the dialog box.

**Table 8-7** The fields in the Add Direct Dial Virtual Entry Queue dialog box

Field	Description
Description	A meaningful description for this VEQ and its IVR experience, such as <i>Direct Dial - English</i> .
VMR entry attempts	The number of times a caller can enter an invalid VMR number before the system rejects the call.
RMX entry queue	The RMX entry queue to use for this VEQ. The drop-down list includes all the RMX entry queues available on the MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.

See also:

[“Shared Number Dialing”](#) on page 190

## Edit Virtual Entry Queue Dialog Box

Lets you edit the virtual entry queue (VEQ) selected on the **Shared Number Dialing** page. The table below describes the fields in the dialog box.

**Table 8-8** The fields in the Edit Virtual Entry Queue dialog box

Field	Description
Virtual entry queue	The VEQ number.
Description	A meaningful description for this VEQ and its IVR experience, such as which language is used.
VMR entry attempts	The number of times a caller can enter an invalid VMR number before the system rejects the call.
RMX entry queue	The RMX entry queue to use for this VEQ. The drop-down list includes all the RMX entry queues available on the MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.

See also:

[“Shared Number Dialing”](#) on page 190

## Edit Direct Dial Virtual Entry Queue Dialog Box

Lets you edit the direct dial virtual entry queue (VEQ). The table below describes the fields in the dialog box.

**Table 8-9** The fields in the Edit Direct Dial Virtual Entry Queue dialog box

Field	Description
Description	A meaningful description for this VEQ and its IVR experience, such as <i>Direct Dial - English</i> .
VMR entry attempts	The number of times a caller can enter an invalid VMR number before the system rejects the call.
RMX entry queue	The RMX entry queue to use for this VEQ. The drop-down list includes all the RMX entry queues available on the MCUs connected to the system, with the number of MCUs that have each entry queue shown in parentheses.

See also:

[“Shared Number Dialing”](#) on page 190



---

# Superclustering

This chapter describes the Polycom® Distributed Media Application™ (DMA™) 7000 system's superclustering capability. It includes the following topics:

- [About Superclustering](#)
- [DMAs](#)
- [Join Supercluster Dialog Box](#)
- [Supercluster Procedures](#)

## About Superclustering

The two-server configuration of the Polycom DMA system is configured as a co-located two-server cluster, which enhances the reliability of the system by providing a measure of redundancy. To provide even greater reliability, geographic redundancy, and better network traffic management, multiple Polycom DMA system *clusters* (either single-server or two-server clusters) in distributed locations can be combined into a *supercluster*.

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

This common data store enables all the Call Servers to share the same site topology, dial plan, bandwidth management, usage reporting, and status monitoring. Up to three of the clusters can be Conference Managers, hosting conference rooms and managing pools of MCUs.

Responsibility for most functionality, including Active Directory and Exchange integration, device registration, call handling, and conference room (VMR) hosting, is apportioned 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.

When you first create a supercluster, it has a single default territory. The cluster that was initially joined to form the supercluster is assigned as the primary cluster for the default territory, and it has no backup cluster. Essentially, one cluster is responsible for everything, and the others do nothing. So immediately after forming a new supercluster, you should reassign territory responsibilities.

#### Note

All the clusters in a supercluster must be running compatible software versions. Patch releases of the same major version will generally be compatible, but major and minor version upgrades will not be compatible. Major and minor version software upgrades of a supercluster take careful planning. See [“Planning a Supercluster Upgrade”](#) on page 329.

If you're planning to form a supercluster, we encourage you to upgrade to the latest version before doing so.

The host names (virtual and physical) of every cluster in the supercluster must be resolvable by all the other clusters. For a superclustered system, A/AAAA records on your DNS server(s) for each physical host name, physical IP address, and virtual host name are mandatory. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

Superclustering is not supported in **Maximum security** mode. See [“The Consequences of Enabling Maximum Security Mode”](#) on page 45.

See also:

[“DMAs”](#) on page 196

[“Supercluster Procedures”](#) on page 200

## DMAs

The **DMAs** page lets you create, view, and manage a *supercluster* of Polycom DMA systems (see [“About Superclustering”](#) on page 195).

If the system you're logged into is not part of a supercluster, the list contains only that system. The **Join Supercluster** command lets you:

- Create a new supercluster by pointing it to another free-standing (not superclustered) Polycom DMA system. Both systems become clusters in the new supercluster. The system you're logged into has its local data store largely replaced by a copy of the data store from the system to which you joined it, and that data becomes the shared supercluster data store.



- Add the system to an existing supercluster by pointing it to one of the existing clusters in the supercluster. The system you're logged into becomes one of the clusters in that supercluster, and its local data store is largely replaced by a copy of the shared supercluster data store.

### Caution

When you add the cluster you're logged into to an existing supercluster, virtually all of that cluster's data and configuration are replaced by the shared data and configuration of the supercluster. This includes, among other things, users, groups, conference rooms, site topology, Conference Manager configuration, Call Server configuration, and integrations.

When you create a new supercluster, the data and configuration of the cluster you're logged into are replaced by the data and configuration of the cluster to which you're pointing it.

Be sure you create a new supercluster by joining the cluster you're logged into to the cluster that has the data and configuration you want to preserve. For instance, if one of the clusters is integrated with your Polycom CMA system, join the other cluster to it, not the other way around.

### Note

You can't add a Polycom CMA system to a supercluster or create a supercluster with a Polycom CMA system. But you can integrate a Polycom DMA system with a Polycom CMA system in order to get site topology and user-to-device association data from the latter (see "[Polycom CMA System Integration](#)" on page 157). You can do this either before or after creating a Polycom DMA supercluster.

If a supercluster exists, the **Remove from Supercluster** command lets you remove the cluster selected in the list from the supercluster, re-initializing 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. The cluster being removed may be either the one you're logged into or another cluster. The system prompts you to confirm. If the cluster you're removing is responsible for any territories (as primary or backup), reassign those territories.

The **Busy Out** command gracefully winds down 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 are 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.

The **Stop Using** command takes the selected cluster immediately out of service:

- 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.

The **Start Using** command puts 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 are 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.

The following table describes the fields on the page.

**Table 9-1** *Fields on the DMAs page*

Column	Description
Host Name	Virtual host name of the cluster's signaling interface.
IP Address	Virtual IP address of the clusters signaling interface.
Model	Type of system. Currently, only DMA 7000 systems may join a supercluster.
Version	Software version of the system.
RAS Port	The UDP port the cluster uses for H.323 RAS (Registration, Admission and Status) signaling.
SIP TCP Port	The TCP port number the cluster uses for SIP.

**Table 9-1** Fields on the DMAs page (continued)

Column	Description
SIP UDP Port	The UDP port number the cluster uses for SIP.
SIP TLS Port	The TLS port number the cluster uses for SIP.
Status	Indicates whether the cluster is superclustered and whether it's in service.
Time	The time and date that the status was checked.

See also:

[“About Superclustering”](#) on page 195

[“Join Supercluster Dialog Box”](#) on page 199

[“Supercluster Procedures”](#) on page 200

## Join Supercluster Dialog Box

In the **Supercluster** page's action list, the **Join Supercluster** command lets you add a Polycom DMA system to an existing supercluster or create a new one. It opens the **Join Supercluster** dialog box, where you can specify any cluster in the supercluster to join. If the cluster you specify isn't already part of an existing supercluster, joining to it creates a new supercluster that gets its shared data store from the cluster you specify.

### Note

All the clusters in a supercluster must be running compatible software versions. Patch releases of the same major version will generally be compatible, but major and minor version upgrades will not be compatible. If the software version of the system you're adding isn't compatible with the supercluster or cluster to which you're joining it, a message tells you so and the join operation is terminated.

The host names (virtual and physical) of every cluster in the supercluster must be resolvable by all the other clusters. For a superclustered system, A/AAAA records on your DNS server(s) for each physical host name, physical IP address, and virtual host name are mandatory. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

The following table describes the fields in the **Join Supercluster** dialog box.

**Table 9-2** *Join Supercluster dialog box*

Column	Description
Host name or IP address	Any existing cluster in the supercluster to which the Polycom DMA system should be joined, or the system with which to form a new supercluster.
User name	An administrator login name for the specified cluster.
Password	The password for the administrator login.

See also:

[“About Superclustering”](#) on page 195

[“DMAs”](#) on page 196

[“Supercluster Procedures”](#) on page 200

## Supercluster Procedures

### To create or join a supercluster

- 1 Go to **Network > DMAs**.
- 2 In the **Actions** list, click **Join Supercluster**.

#### Note

You can only add one cluster to a supercluster at a time. Wait until the current join operation is completely finished before attempting to add another cluster to the supercluster.

- 3 In the **Join Supercluster** dialog box, do one of the following:
  - To create a new supercluster, enter the host name or IP address of the other Polycom DMA cluster with which to form the supercluster. Be sure the other cluster is the one whose data store you want shared with the supercluster.
  - To add this system to an existing supercluster, enter the host name of one of the clusters in the supercluster.

**Note**

You may specify an IP address instead, but the host names (virtual and physical) of every cluster in the supercluster must be resolvable by all the other clusters. For a superclustered system, A/AAAA records on your DNS server(s) for each physical host name, physical IP address, and virtual host name are mandatory. See [“Add Required DNS Records for the Polycom DMA System”](#) on page 18.

- 4 Enter the user name and password with which to log into the Polycom DMA cluster you specified.

- 5 Click **OK**.

A prompt warns you that the system will restart and local data will be overwritten, and asks you to confirm.

- 6 Click **Yes**.

The cluster you’re logged into connects to the cluster you specified and establishes or joins the supercluster. It obtains supercluster-wide configuration and data (this may take a few minutes). A dialog box informs you when the process is complete and the cluster is ready to restart. Shortly after that, the cluster logs you out and restarts.

- 7 Click **OK** to log out immediately, or simply wait.

**Note**

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

- 8 Log back in and verify that the **Supercluster Status** pane of the **Dashboard** shows the correct number of servers and clusters, and there are no warnings.
- 9 Go to **Network > DMAs**, verify that the status of each DMA cluster is *Superclustered*, and reassign territory responsibilities as needed.

**To remove a cluster from the supercluster****Note**

If possible, remove a cluster only while its server or servers are on line. If you must remove a cluster while one or both servers are off line, be aware that an offline server will be in an inconsistent state when it’s brought back on line. The only supported procedure for fixing a server in this state is to re-install it from media.

- 1 Make sure that there are no calls on the cluster, and that all of its MCUs are out of service. See [“MCU Procedures”](#) on page 124.
- 2 Reassign all of the cluster’s territory responsibilities to a different cluster.

- 3** Go to **Network > DMAs**. In the list, select the cluster you want to remove.
- 4** In the **Actions** list, select **Remove from Supercluster**.
- 5** When asked to confirm that you want to remove the cluster, click **Yes**.  
The selected cluster is removed from the supercluster. A dialog box informs you when the process is complete. If the cluster you removed is the one you're logged into, it logs you out and restarts.
- 6** Click **OK** to log out immediately, or simply wait.

**Note**

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

- 7** Log into the system you removed and verify on the **Supercluster Status** pane of the **Dashboard** that the system is no longer superclustered.

See also:

["About Superclustering"](#) on page 195

["DMAs"](#) on page 196

["Join Supercluster Dialog Box"](#) on page 199

---

# Call Server Configuration

This chapter describes the Polycom® Distributed Media Application™ (DMA™) 7000 system's configuration tools and tasks related to its Call Server:

- [About the Call Server Capabilities](#)
- [Call Server Settings](#)
- [Domains](#)
- [Dial Rules](#)
- [Hunt Groups](#)
- [Device Authentication](#)
- [Registration Policy](#)
- [Prefix Service](#)
- [Embedded DNS](#)

These are settings and features that are shared across superclustered systems. See ["Introduction to the Polycom DMA System"](#) on page 1.

## About the Call Server Capabilities

The Polycom DMA system's Call Server capabilities provide:

- Gatekeeper functionality (if H.323 signaling is enabled)
- SIP proxy server and registrar functionality (if SIP signaling is enabled)
- XMPP server (if XMPP signaling is enabled)
- Bandwidth management.
- H.323 <-> SIP gateway

In addition, the system can be integrated with a Juniper Networks Service Resource Controller (SRC) to provide bandwidth assurance services.

**Note**

SIP and XMPP signaling are not supported in **Maximum security** mode. See [“The Consequences of Enabling Maximum Security Mode”](#) on page 45.

Call server configuration begins with enabling the desired signaling on each cluster’s [Signaling Settings](#) page. Other Call Server settings are shared across all systems in a supercluster and set on the **Admin > Call Server** pages.

**Note**

In an IPv4 + IPv6 environment, the Polycom DMA system gatekeeper prefers the IPv4 address for devices that register with both.

For example, if endpoint A is a dual-stack device (that is, it supports both IPv4 and IPv6) and registers over IPv6 to a Polycom DMA system that’s also dual-stack, the RRQ (Registration Request) message informs the DMA gatekeeper of the endpoint’s IPv6 and IPv4 addresses (as well as its E.164 alias, etc.).

If endpoint A dials the E.164 address of another dual-stack endpoint (endpoint B), DMA gives preference to the IPv4 address by sending endpoint B’s IPv4 address in the ACF (Admission Confirm) message to endpoint A.

Even though the initial ARQ and corresponding ACF were over IPv6, the expected behavior is that endpoint A will continue the H.323 signaling session to endpoint B over IPv4 since the DMA gatekeeper informed endpoint A of endpoint B’s IPv4 signaling IP.

See also:

[“Call Server Configuration”](#) on page 203

[“Call Server Settings”](#) on page 205



## Call Server Settings

On the **Call Server Settings** page, you can specify certain gatekeeper and SIP proxy settings used by the Polycom DMA system Call Server. These settings are shared across the supercluster and apply to all the clusters.

The following table describes the fields on the page.

**Table 10-1** Fields on the Call Server Settings page

Field	Description
Allow site-less registrations	If this option is selected, endpoints that don't belong to a site or territory can register with the supercluster gatekeeper or SIP proxy. Otherwise, only endpoints in a subnet configured in the site topology can register.
Accept H.323 neighbor requests only from specified external gatekeepers	If this option is selected, the system accepts H.323 location requests (LRQs) only from gatekeepers configured on <b>External Gatekeeper</b> page (see <a href="#">"External Gatekeeper"</a> on page 82).
Resolve H.323 Email-ID dial strings to other registered H.323 aliases	If this option is selected, the system 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 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).
Allow calls to/from rogue endpoints	If this option is selected, the system permits rogue endpoints to place and receive calls.  Turning this option off blocks calls from and to endpoints that are in sites managed by the system, but are not registered and active.  This option has no effect on other unregistered network devices (such as MCUs, GKs, and SBCs).
Gatekeeper call mode	<b>Direct call mode</b> — The gatekeeper processes only H.225.0 RAS call control messages. The endpoints exchange other call signaling and media control messages directly, bypassing the gatekeeper.  <b>Routed call mode</b> — The gatekeeper proxies all H.323 signaling messages.

**Table 10-1** Fields on the Call Server Settings page (continued)

Field	Description
Available bandwidth limit (percent)	<p>Sets the maximum percentage of the available bandwidth that can be allocated to a single call.</p> <p>If the requested bandwidth exceeds this value, the gatekeeper “downspeeds” (reduces the bit rate of) the call, but only to the user’s downspeed minimum.</p> <p>If there is insufficient bandwidth to comply with both this setting and the downspeed minimum, the call is rejected.</p>
Location request hop count	The initial hop count the gatekeeper 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.
Registration refresh interval (seconds)	<p>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.</p> <p>For SIP endpoints, specifies the refresh interval used if the endpoint didn’t specify an interval or specified one greater than this value.</p> <p>Must be greater than or equal to the minimum SIP registration interval and in the range 150-9999.</p>
Minimum SIP registration interval (seconds)	<p>The minimum time between “keep alive” messages to SIP endpoints.</p> <p>Must be less than or equal to the registration refresh interval and in the range 150-3600.</p>
IRQ sending interval (seconds)	<p>The interval at which the system sends IRQ messages to H.323 endpoints in a call, requesting QoS (quality of service) reports.</p> <p>Must be in the range 10-600.</p>
SIP peer timeout (seconds)	<p>The timeout value for calls to peer proxy servers, after which the dial attempt is canceled.</p> <p>Must be in the range 3-300.</p>
Territory failover delay (seconds)	<p>The number of seconds a territory’s backup supercluster node waits after losing contact with the primary before it takes over the territory.</p> <p>Must be in the range 6-300.</p>
Timeout for call forwarding when no answer (seconds)	<p>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.</p> <p>Must be in the range 5-32.</p>

See also:

[“Call Server Configuration”](#) on page 203

[“About the Call Server Capabilities”](#) on page 203

## Domains

On the **Domains** page, you can add administrative domains to or remove them from the list of domains from which registrations are accepted.

If the 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.

### Note

The *Resolve to external address* dial rule action (see [“Add Dial Rule Dialog Box”](#) on page 212) 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 won't match any dial string and can't be used.

The following table describes the fields on the page.

**Table 10-2** *Fields on the Domains page*

Field	Description
Add new domain	<p>Enter a domain and click <b>Add</b> to add it to the <b>Authorized domains</b> list.</p> <p>Domain names must be valid and full domains, but you can replace a single host label within a domain with the wildcard character to match multiple subdomains. For instance, *.mycompany.com matches:</p> <p style="padding-left: 40px;">eng.mycompany.com fin.mycompany.com</p> <p>And eng.*.mycompany.com matches:</p> <p style="padding-left: 40px;">eng.sanjose.mycompany.com eng.austin.mycompany.com</p>
Authorized domains	<p>The list of domains from which the system accepts registrations. Select a domain and click <b>Remove</b> to remove it from the list.</p> <p>Click <b>Restore Defaults</b> to remove all domains so that the system accepts registrations from any domain.</p>

**Table 10-2** *Fields on the Domains page (continued)*

Field	Description
Locally registered SIP endpoints belong to every local domain	Specifies that call requests for locally registered SIP endpoints don't have to match the domain. For example, if there is an endpoint registered as 'sip:johnsmith@1.1.1.1' and this option is enabled, a call to 'sip:johnsmith@mycompany.com' may be connected to that endpoint.  If this option is not selected, call requests must exactly match the URI of the registered endpoint.
Email IDs of locally registered H.323 endpoints belong to every local domain	Specifies that call requests for locally registered H.323 endpoints' email IDs don't have to match the domain. For example, if there is an endpoint registered as 'h323:johnsmith@1.1.1.1' and this option is enabled, a call to 'h323:johnsmith@mycompany.com' may be connected to that endpoint.  If this option is not selected, call requests must exactly match the URI of the registered endpoint.

See also:

[“Call Server Configuration”](#) on page 203

[“About the Call Server Capabilities”](#) on page 203

## Dial Rules

Dial rules specify how the Polycom DMA system Call Server uses the dial string to determine where to route the call. This 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 Polycom DMA system Call Server receives a call request and associated dial string, it applies the first matched (highest priority) dial rule.

The Call Server comes with a default dial plan installed that provides the most commonly needed address resolution processing. On the **Dial Rules** page, you can add, edit, remove, and change the order of the dial rules that make up the system's dial plan. This is a supercluster-wide configuration.

The following table describes the fields in the list.

**Table 10-3** *Fields in the Dial Rules list*

Column	Description
Order	The priority order of the rules. Use the <b>Move Up</b> and <b>Move Down</b> commands to change the priority of a rule.
Description	Brief description of the rule.
Action	Action performed by the rule.
Preliminary Enabled	Indicates whether a script filters or transforms the dial string before the action is performed.
Enabled	Indicates whether the rule is turned on.

See also:

[“Call Server Configuration”](#) on page 203

[“The Default Dial Plan and Suggestions for Modifications”](#) on page 209

[“Add Dial Rule Dialog Box”](#) on page 212

[“Edit Dial Rule Dialog Box”](#) on page 214

## The Default Dial Plan and Suggestions for Modifications

The Polycom DMA system is configured by default with a generic dial plan that covers many common scenarios and may prove adequate for your needs. It's described in the table below.

**Table 10-4** *How the default dial plan works*

Rule	Effect
1 Dial registered endpoints by alias	If the dial string is the alias or SIP URI of a registered endpoint, the call is routed to that endpoint.
2 Dial by conference room ID	Otherwise, if the dial string is the dial-in number of a conference room on the Polycom DMA system, the call is routed to that conference room.
3 Dial by virtual entry queue ID	Otherwise, if the dial string is the dial-in number of a virtual entry queue on the Polycom DMA system, the call is routed to that VEQ.

**Table 10-4** How the default dial plan works (continued)

Rule	Effect
4 Dial services by prefix	<p>Otherwise, 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.</p> <p><b>Note:</b> For a SIP peer, the dial string must 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: 123alice</p>
5 Dial external networks by H.323 URL, email ID, or SIP URI	<p>Otherwise, if the address is an external address, the call is routed to that external address (H.323 calls use an SBC to reach IP addresses outside the enterprise network).</p> <p>Examples of external addresses: H323:johnsmith@someothercompany.com sip:johnsmith@someothercompany.com</p>
6 Dial endpoints by IP address	<p>Otherwise, if the address is an IP address, the call is routed to that IP address (H.323 calls use an SBC to reach IP addresses outside the enterprise network).</p> <p>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</p>

If you have special configuration needs and want to modify the 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.

Here are some suggestions and guidelines for modifying the dial plan:

- To add an MCU, ISDN gateway, SBC, neighbor gatekeeper, peer SIP proxy, 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 Rule 4 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. But note that Rule 6 (*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.

- 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 another SIP proxy and you want to route calls to that peer proxy 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 (see [“Add External SIP Peer Dialog Box”](#) on page 89).

When routing to a peer proxy, the Polycom 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.

- 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 ten digits long, you may want to route calls to that gatekeeper only if the dial string begins with a certain prefix followed by exactly ten 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 ten 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 address** action with a preliminary script that transforms the string 7xxxx to H323:xxxx@enterprisepartner.com.

See also:

[“Dial Rules”](#) on page 208

[“Add Dial Rule Dialog Box”](#) on page 212

[“Edit Dial Rule Dialog Box”](#) on page 214

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“Sample Preliminary and Postliminary Scripts”](#) on page 216

## Add Dial Rule Dialog Box

The following table describes the fields in the **Add Dial Rule** dialog box.

**Table 10-5** Add Dial Rule dialog box

Field	Description
<b>Dial Rule</b>	
Description	The text description displayed on the <b>Dial Rules</b> page.
Action	The action to be performed. When you select some actions, additional settings become available. See the table below for more information about the actions.
Enabled	Clearing this check box lets you turn off a rule without deleting it.
<b>Preliminary</b>	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.  <a href="#">"Sample Preliminary and Postliminary Scripts"</a> on page 216 provides some examples you can experiment with and modify for your purposes.
Enabled	Lets you turn a preliminary on or off without deleting it.
Script	Type (or paste) the preliminary script you want to apply. Then click <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

The following table describes the **Action** options and how the system attempts to resolve the destination address (dial string) for each.

**Table 10-6** Dial rule actions

For this action:	The system attempts to resolve the address as follows:
Block	Blocks the call.
Resolve to IP address	Tries to treat the dial string as an IP address, and if it can, assumes that it's the address of an unregistered endpoint.
Resolve to registered endpoint	Looks for a registered endpoint (active or inactive) that has the same alias or signaling address.



**Table 10-6** *Dial rule actions (continued)*

For this action:	The system attempts to resolve the address as follows:
Resolve to service prefix	Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present).  <b>Note:</b> For a SIP peer, the dial string must 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:  123alice
Resolve to external SIP peer	Checks the domain of the dial string against all of the rule's selected proxies, looking for a peer proxy responsible for that domain.
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.
Resolve to external address	Determines if the dial string is a well-formed instance of an enabled external address type, and if so, applies the resolution procedures specified in the applicable standard for that address type.
Resolve to conference room ID	Looks for a conference room or virtual meeting room that matches the dial string.
Resolve to virtual entry queue	Looks for a shared-number entry queue that matches the dial string.

See also:

[“Dial Rules”](#) on page 208

[“The Default Dial Plan and Suggestions for Modifications”](#) on page 209

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“Sample Preliminary and Postliminary Scripts”](#) on page 216

## Edit Dial Rule Dialog Box

The following table describes the fields in the **Edit Dial Rule** dialog box.

**Table 10-7** *Edit Dial Rule dialog box*

Field	Description
<b>Dial Rule</b>	
Description	The text description displayed on the <b>Dial Rules</b> page.
Action	The action to be performed. When you select some actions, additional settings become available. See the table below for more information about the actions.
Enabled	Clearing this check box lets you turn off a rule without deleting it.
<b>Preliminary</b>	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.  <a href="#">"Sample Preliminary and Postliminary Scripts"</a> on page 216 provides some examples you can experiment with and modify for your purposes.
Enabled	Lets you turn a preliminary on or off without deleting it.
Script	Type (or paste) the preliminary script you want to apply. Then click <b>Debug this script</b> to open the <a href="#">Script Debugging Dialog Box for Preliminaries/Postliminaries</a> and test the script with various variables.

The following table describes the **Action** options and how the system attempts to resolve the destination address (dial string) for each.

**Table 10-8** *Dial rule actions*

For this action:	The system attempts to resolve the address as follows:
Block	Blocks the call.
Resolve to IP address	Tries to treat the dial string as an IP address, and if it can, assumes that it's the address of an unregistered endpoint.
Resolve to registered endpoint	Looks for a registered endpoint (active or inactive) that has the same alias or signaling address.
Resolve to service prefix	Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present).
Resolve to external SIP peer	Checks the domain of the dial string against all of the rule's selected proxies, looking for a peer proxy responsible for that domain.

**Table 10-8** *Dial rule actions (continued)*

For this action:	The system attempts to resolve the address as follows:
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.
Resolve to external address	Determines if the dial string is a well-formed instance of an enabled external address type, and if so, applies the resolution procedures specified in the applicable standard for that address type.
Resolve to conference room ID	Looks for a conference room or virtual meeting room that matches the dial string.
Resolve to virtual entry queue	Looks for a shared-number entry queue that matches the dial string.

See also:

[“Dial Rules”](#) on page 208

[“The Default Dial Plan and Suggestions for Modifications”](#) on page 209

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“Sample Preliminary and Postliminary Scripts”](#) on page 216

## Script Debugging Dialog Box for Preliminaries/Postliminaries

The **Script Debugging** dialog box lets you test a Javascript executable script that you've added as preliminary to a dial rule or as a postliminary for an external gatekeeper, SIP peer, or SBC. It lets you specify parameters of a call and the dial string, and see what effect the script has on the dial string.

The following table describes the fields in the **Script Debugging** dialog box.

**Table 10-9** *Script Debugging dialog box*

Field	Description
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. Then click <b>Execute Script</b> . <b>Note:</b> 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 in order to set the first four caller variables.
Caller variables	Lists variables that can be used in the script to represent caller values. Click an item in the <b>Variable Value</b> column to enter a value to test for that variable.

**Table 10-9** *Script Debugging dialog box (continued)*

Field	Description
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 (e.g., <code>println</code> statements).
Output SIP headers	For an external SIP peer's postliminary, displays the headers produced by the script.

See also:

[“Dial Rules”](#) on page 208

[“External Gatekeeper”](#) on page 82

[“External SIP Peer”](#) on page 88

[“External SBC”](#) on page 106

[“Sample Preliminary and Postliminary Scripts”](#) on page 216

## 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, or SBC).

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.

```
////////////////////////////////////
// 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
// SIP:1234@abc.com --> sip:991234@abc.com
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.
//
println("DIAL_STRING: " + DIAL_STRING);
println("CALLER_SITE_NAME: " + CALLER_SITE_NAME);
println("CALLER_SITE_COUNTRY_CODE: " + CALLER_SITE_COUNTRY_CODE);
println("CALLER_SITE_AREA_CODE: " + CALLER_SITE_AREA_CODE);
println("CALLER_SITE_DIGITS: " + CALLER_SITE_DIGITS);
println("CALLER_H323ID: " + CALLER_H323ID);
println("CALLER_E164: " + CALLER_E164);
println("CALLER_TEL_URI: " + CALLER_TEL_URI);
println("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:([^@]*)@.*/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";
}

```

See also:

[“Dial Rules”](#) on page 208

[“Script Debugging Dialog Box for Preliminaries/Postliminaries”](#) on page 215

[“External Gatekeeper”](#) on page 82

[“External SIP Peer”](#) on page 88

[“External SBC”](#) on page 106

## Hunt Groups

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 Polycom 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 the BUSY message to the caller.

### Note

Hunt group calls don't invoke the Call Server's H.323-SIP gateway function. If an endpoint using one signaling type calls a hunt group, and the selected hunt group member is of the other signaling type, the call fails.

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.

The **Hunt Groups** page lists the defined hunt groups and lets you add, edit, and delete hunt groups.

The following table describes the fields in the list.

**Table 10-10** *Fields in the Hunt Groups list*

Column	Description
Name	Hunt group name.
Description	Brief description of the hunt group.
Aliases	The aliases (dial strings) that resolve to this hunt group.
Members	The endpoints included in the hunt group.
Enabled	Indicates whether the hunt group is being used.

See also:

["Call Server Configuration"](#) on page 203

["Add Hunt Group Dialog Box"](#) on page 221

["Edit Hunt Group Dialog Box"](#) on page 221



## Add Hunt Group Dialog Box

The **Add Hunt Group** dialog box lets you define a new hunt group in the system and add members to it. The following table describes the fields in the dialog box.

**Table 10-11** Add Hunt Group dialog box

Field	Description
<b>General Info</b>	
Name	Hunt group name.
Description	The text description displayed in the <b>Hunt Groups</b> list.
Enabled	Clearing this check box lets you define a new hunt group without putting it immediately into service.
No answer timeout	Number of seconds to wait for a hunt group member to answer a call before giving up and trying another member.
Aliases	Lists the aliases (dial strings) that resolve to this hunt group. Click <b>Add</b> to add an alias. Click <b>Edit</b> or <b>Delete</b> to change or remove the selected alias.
<b>Hunt Group Members</b>	
Search members	Search for endpoints by name or IP address.
Available members	Lists the endpoints that match the search criteria.
Selected members	Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to another.

See also:

[“Hunt Groups”](#) on page 220

[“Add Alias Dialog Box”](#) on page 222

[“Edit Alias Dialog Box”](#) on page 223

## Edit Hunt Group Dialog Box

The **Edit Hunt Group** dialog box lets you modify the selected hunt group and add or remove members. The following table describes the fields in the dialog box.

**Table 10-12** Edit Hunt Group dialog box

Field	Description
<b>General Info</b>	
Name	Hunt group name.
Description	The text description displayed in the <b>Hunt Groups</b> list.
Enabled	Clearing this check box lets you stop using a hunt group without deleting it.
No answer timeout	Number of seconds to wait for a hunt group member to answer a call before giving up and trying another member.
Aliases	Lists the aliases (dial strings) that resolve to this hunt group. Click <b>Add</b> to add an alias. Click <b>Edit</b> or <b>Delete</b> to change or remove the selected alias.
<b>Hunt Group Members</b>	
Search members	Search for endpoints by name or IP address.
Available members	Lists the endpoints that match the search criteria.
Selected members	Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to another.

See also:

[“Hunt Groups”](#) on page 220

[“Add Alias Dialog Box”](#) on page 222

[“Edit Alias Dialog Box”](#) on page 223

## Add Alias Dialog Box

The **Add Alias** dialog box lets you add an alias value to the hunt group. Enter the alias in the **Value** box and click **OK**.

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.

See also:

[“Hunt Groups”](#) on page 220

[“Add Hunt Group Dialog Box”](#) on page 221

[“Edit Hunt Group Dialog Box”](#) on page 221

## Edit Alias Dialog Box

The **Edit Alias** dialog box lets you change an alias value assigned to the hunt group. Edit the alias in the **Value** box and click **OK**.

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.

See also:

[“Hunt Groups”](#) on page 220

[“Add Hunt Group Dialog Box”](#) on page 221

[“Edit Hunt Group Dialog Box”](#) on page 221

## Device Authentication

Device authentication enhances security by requiring devices registering with or calling the Polycom DMA system to provide credentials that the system can authenticate. In turn, the Polycom 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 FQDN, allowing each cluster in a supercluster to have its own realm for challenges.

The **Device Authentication** page has two tabs, **Inbound Authentication** and **Shared Outbound Authentication**.

### Inbound Authentication

On the **Inbound Authentication** tab, you can:

- Turn on H.235 authentication for H.323 devices.
- Turn on and configure SIP digest authentication for SIP devices.
- Maintain the Call Server’s local inbound device authentication list.

#### Note

You can turn inbound authentication off and on for specific devices (assuming that it’s turned on here at the system level for that device type). See [“Endpoints”](#) on page 73.

### Inbound 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 Polycom DMA system authenticates requests as follows:

- If the request is a signaling request (ARQ, BRQ, DRQ) from an unregistered endpoint, the Call Server doesn't authenticate the credentials.
- If the request is 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.

### Inbound SIP Device Authentication

The SIP digest authentication mechanism is described in RFC 3261, starting in section 22, page 192, and in RFC 2617 section 3, page 5). When a SIP endpoint calls the Polycom DMA system, if the request includes authentication information, that information is checked against the Call Server's local device authentication list, which you create on this page.

If SIP authentication is enabled and an endpoint's request doesn't include authentication information, the Call Server responds with an authentication challenge (a 401 or 407 response, depending on how you configure it) containing the required fields (see RFCs). If the endpoint responds with valid authentication information, the system accepts the call.

### Shared Outbound Authentication

On the **Shared Outbound Authentication** tab, you can maintain the Call Server's general list of authentication credentials, which it uses to authenticate itself to external SIP peers for which the appropriate device-specific credentials haven't been defined.

When you add an external SIP peer, you can specify whether the Call Server handles challenges (401 and 407) or passes them to the source of the call, and you can define authentication credentials specifically for that SIP peer. See ["Add External SIP Peer Dialog Box"](#) on page 89.

#### Note

For H.323, when you add a neighbor gatekeeper, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper. See ["Add External Gatekeeper Dialog Box"](#) on page 84.

The following table describes the fields on the **Device Authentication** page.

**Table 10-13** Fields on the Device Authentication page

Field	Description
<b>Inbound Authentication</b>	
Enable H.323 device authentication	Check the box and click <b>Update</b> to turn on H.323 device authentication.
Enable SIP device authentication	Check the box, configure the fields below, and click <b>Update</b> to turn on SIP device authentication.
Use default realm	This option, the default, sets the realm for the Call Server to the cluster's FQDN (allowing each cluster of a supercluster to have its own realm). Clear the check box to change the string in the <b>Realm</b> field.
Realm	The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally includes the host or domain name of the Call Server. See RFC 2617 and RFC 3261.
Enable proxy authentication	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).
Authentication valid time (seconds)	Specifies the time period within which the Call Server doesn't re-challenge a device that previously authenticated itself.
Name	Lists the devices in the system's device authentication list. Use the <b>Search names</b> field and <b>Search</b> button above the list to narrow the list. The system finds devices whose names begin with the search string.
<b>Shared Outbound Authentication</b>	
(table of authentication entries)	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 <b>Realm</b> or <b>Name</b> field and <b>Search</b> 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 (see <a href="#">"Edit External SIP Peer Dialog Box"</a> on page 92). If there is none with the correct realm, it looks at the entries listed here.

See also:

[“Call Server Configuration”](#) on page 203

[“Add Device Authentication Dialog Box”](#) on page 226

[“Edit Device Authentication Dialog Box”](#) on page 226

[“Add Authentication Dialog Box”](#) on page 103

[“Edit Authentication Dialog Box”](#) on page 103

## Add Device Authentication Dialog Box

The **Add Device Authentication** dialog box appears when you click **Add** on the **Device Authentication** page while the **Inbound Authentication** tab is selected. It lets you add a device’s authentication credentials to the list of device credential entries against which the Call Server checks a device’s credentials.

The following table describes the fields in the **Add Device Authentication** dialog box.

**Table 10-14** Add Device Authentication dialog box

Field	Description
<b>Device Authentication</b>	
Name	The name that the device includes in registration and signaling requests or responses to authentication challenges.  <b>Note:</b> 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 Confirm password	The password that the device includes in registration and signaling requests or responses to authentication challenges.

See also:

[“Device Authentication”](#) on page 223

## Edit Device Authentication Dialog Box

The **Edit Device Authentication** dialog box appears when you click **Edit** on the **Device Authentication** page while an entry on the **Inbound Authentication** tab is selected. It lets you edit the authentication credentials for the selected device.

The following table describes the fields in the **Edit Device Authentication** dialog box.

**Table 10-15** *Edit Device Authentication dialog box*

Field	Description
<b>Device Authentication</b>	
Name	The name that the device includes in registration and signaling requests or responses to authentication challenges.  <b>Note:</b> 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 Confirm password	The password that the device includes in registration and signaling requests or responses to authentication challenges.

See also:

[“Device Authentication”](#) on page 223

## Registration Policy

On the **Registration Policy** page, you can specify policies to control registration by endpoints. To do so, you define the following:

- **Compliance policy:** Write an executable script (using the Javascript language) that specifies the criteria for determining whether an endpoint is *compliant* or *noncompliant* with the registration policy.
- **Admission policy:** Select the action to be taken when an endpoint is compliant, and the action to be taken when an endpoint is noncompliant.

The actions that may be taken are:

*Accept registration* – The endpoint's registration request is accepted and its status becomes *Active* (see [“Endpoints”](#) on page 73 for more information about endpoint status values).

*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. Their status remains unchanged until you manually unblock them.

*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 (see [“Call Server Settings”](#) on page 205). If the endpoint sends another registration request, the registration policy is applied to that request.

*Quarantine registration* – The endpoint's registration request is accepted, but its status becomes *Quarantined*. It can't make or receive calls. The system processes registration attempts (and unregistration attempts) from quarantined endpoints, but doesn't apply the registration policy. Their status remains either Quarantined if registered or Quarantined (Inactive) if unregistered until you manually remove them from quarantine.

You can also specify whether the policy is to be applied only to new registrations, or also to re-registrations with changed properties.

The following table describes the fields on the page.

**Table 10-16** *Fields on the Registration Policy page*

Field	Description
When compliant	Select the action to take when the registration policy script returns COMPLIANT.
When noncompliant	Select the action to take when the registration policy script returns NONCOMPLIANT.
Policy Applies	Select whether to apply the registration policy script only to new registrations or also to changed re-registrations. If you choose the latter, you can optionally select <b>Ignore IP and port changes</b> so that the registration policy script is not applied if those are the only changes.
Registration policy compliance script	Type (or paste) the registration policy script you want to apply. Then click <b>Debug this script</b> to test the script with various variables. Click <b>Reapply policy</b> to run the script now, applying any policy changes you've made to existing registered endpoints.
Inactive registration deletion days	Select to specify that endpoints whose status is <i>Inactive</i> (that is, their registrations have expired) are deleted from the system after the specified number of days.

See also:

[“Call Server Configuration”](#) on page 203

[“Registration Policy Scripting”](#) on page 229

[“Script Debugging Dialog Box for Registration Policy Scripts”](#) on page 231

[“Sample Registration Policy Scripts”](#) on page 231

[“Endpoints”](#) on page 73



## Registration Policy Scripting

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. The script can specify any number of criteria, and they can be as broad or narrow as you want.

A script can return COMPLIANT or NONCOMPLIANT. The corresponding settings on the **Registration Policy** page let you specify what action to take for each of these return values.

A script can also assign a value (up to 100 characters) to the EP\_EXCEPTION variable. This variable's initial value is blank (empty string). Assigning a non-blank value to it causes an *exception* to be recorded for the endpoint being processed. Exceptions appear on the **Endpoints** page, and you can search for endpoints with exceptions. See "[Endpoints](#)" on page 73.

Exceptions can serve a variety of purposes, from specifying the reason a registration was rejected to simply recording some useful information about the registration request for future reference. For instance, you may want all endpoints to conform to a specific alias dial string pattern, but not want to quarantine those that don't comply. Assigning an exception to non-compliant endpoints allows you to find them on the **Endpoints** page so that you can contact the owners.

See "[Sample Registration Policy Scripts](#)" on page 231 for some examples.

The following table describes the other 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).

**Table 10-17** Predefined variables for registration policy scripts

Variable	Initial value
EP_REG_IS_H323	"TRUE" if the registration request uses H.323 signaling. Blank otherwise.
EP_REG_IS_SIP	"TRUE" if the registration request uses SIP signaling. Blank otherwise.
EP_IP	Array containing endpoint IP address. 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.
EP_IS_IPV4	"TRUE" if EP_IP is an IPv4 address. Blank otherwise.
EP_IS_IPV6	"TRUE" if EP_IP is an IPv6 address. Blank otherwise.
EP_SIP_SIP_URI_ALIAS	Endpoint alias value associated with SIP sip: URI or blank.

**Table 10-17** Predefined variables for registration policy scripts (continued)

Variable	Initial value
EP_SIP_TEL_URI_ALIAS	Endpoint alias value associated with SIP TEL: URI or blank.
EP_SIP_SIPS_URI_ALIAS	Endpoint alias value associated with SIP SIPS: URI or blank.
EP_H323_DIALEDDIGITS_ALIAS	Endpoint alias value associated with H.323 dialedDigits or blank.
EP_H323_H323_ID_ALIAS	Endpoint alias value associated with H.323 H323-ID or blank.
EP_H323_URL_ID_ALIAS	Endpoint alias value associated with H.323 URL-ID or blank.
EP_H323_TRANSPORTID_ALIAS	Endpoint alias value associated with H.323 transportID or blank.
EP_H323_EMAIL_ID_ALIAS	Endpoint alias value associated with H.323 email-ID or blank.
REG_IS_PERMANENT	“TRUE” if endpoint is already permanently registered. Blank otherwise.
EP_MODEL	Endpoint model.
EP_VERSION	Endpoint software version number.
EP_OWNER	Endpoint owner.
EP_OWNER_DOMAIN	Endpoint owner's domain.
REG_SITE_NAME	Site where endpoint is attempting to register.
REG_SITE_COUNTRY_CODE	Country code of the site where the endpoint is attempting to register.
REG_SITE_AREA_CODE	Area code of the site where the endpoint is attempting to register.
REG_SITE_DIGITS	Number of digits in the subscriber number configured for the site where the endpoint is attempting to register.
REG_SUBNET_IP_ADDRESS	Array containing the IP address of the subnet where the endpoint is attempting to register.
REG_SUBNET_MASK	Array containing the IP mask of the subnet where the endpoint is attempting to register.

See also:

[“Registration Policy”](#) on page 227

[“Script Debugging Dialog Box for Registration Policy Scripts”](#) on page 231

[“Sample Registration Policy Scripts”](#) on page 231

## Script Debugging Dialog Box for Registration Policy Scripts

When you click **Debug this script** on the **Registration Policy** page, the **Script Debugging** dialog box appears, in which you can test your script.

The dialog box lets you enter or select test values for the predefined variables (see [“Registration Policy Scripting”](#) on page 229 for a list of these).

The **Script output** box displays any output produced by the script when it runs (e.g., `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 also displays that.

Testing your script is an iterative process. Specify test values for the variables used in your script. Then click **Run Script** to see the results of applying the script using those variable values. Repeat as often as necessary, using different variable values.

If necessary, make changes to your script and then test some more, until you're satisfied that the script accomplishes what you intended.

See also:

[“Registration Policy”](#) on page 227

[“Registration Policy Scripting”](#) on page 229

[“Sample Registration Policy Scripts”](#) on page 231

## 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. See [“Registration Policy Scripting”](#) on page 229 for more information.

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.

```

////////////////////////////////////
// Reject SIP Registrations
//
if (!EP_REG_IS_H323) return NONCOMPLIANT;

////////////////////////////////////
// Reject aliases that aren't the right length otherwise accept!
// IF REG_SITE_COUNTRY_CODE = 1
//   AND IF REG_SITE_AREA_CODE = 303
//   AND IF REG_SITE_DIGITS = 4
// AND IF EP_H323_DIALEDDIGITS_ALIAS[0].length() != 8
// return NONCOMPLIANT;
//
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 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].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;

```

```
whitelist = new Array(
    "10.20.30.40",
    "192.168.3.14",
    "192.168.174.233"
);

if (EP_IS_IPV4) {
    nparts = 4;
}

for (i = 0; i < nparts; i++)
{
    if (i == 0)
    {
        IPstring = EP_IP[i];
    }
    else
    {
        IPstring += "." + EP_IP[i]
    }
}

for (i=0; i < whitelist.length; i++)
{
    if (IPstring == whitelist[i]) {
        return COMPLIANT;
    }
}

return NONCOMPLIANT;
```

See also:

["Registration Policy" on page 227](#)

["Registration Policy Scripting" on page 229](#)

["Script Debugging Dialog Box for Registration Policy Scripts" on page 231](#)

## Prefix Service

The **Prefix Service** page provides a complete list of all configured prefixes in one place, so you can easily determine what prefixes are in use and whether any conflicts exist.

For your convenience, its **Actions** list lets you add, edit, or delete any of the devices without having to navigate back to the specific page for that device type. It also lets you add, edit, or delete simplified gateway dialing services (see [“Add Simplified Gateway Dialing Prefix Dialog Box”](#) on page 235).

The following table describes the fields in the list.

**Table 10-18** *Fields in the Prefix Service list*

Column	Description
Service/Device Name	The name of the service or device assigned the specified prefix(es). Devices with no prefix(es) assigned are listed, but shown as disabled.
Prefix Range	The dial string prefix(es) assigned to this service or device.
Service/Device Type	Type of service or device.
Description	Brief description of the service or device.
Enabled	Indicates whether the service or device is enabled or disabled.

See also:

[“Call Server Configuration”](#) on page 203

[“Add Simplified Gateway Dialing Prefix Dialog Box”](#) on page 235

[“Edit Simplified Gateway Dialing Prefix Dialog Box”](#) on page 235

## Add Simplified Gateway Dialing Prefix Dialog Box

The **Add Simplified Gateway Dialing Prefix** dialog box lets you create a new prefix-driven simplified gateway dialing service.

The following table describes the fields in the dialog box.

**Table 10-19** Fields in the Add Simplified Gateway Dialing Prefix dialog box

Column	Description
Name	A display name for this service.
Description	Brief description of the service.
Enabled	Clearing this check box lets you turn off the service without deleting it.
Simplified dialing prefix	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 <i>Dial services by prefix</i> 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.
Use all gateways	Indicates whether this service applies to all available gateways or only those selected below.
Available gateways	Lists the gateways that have at least one session profile specifying an H.320 or PSTN protocol. See <a href="#">"Edit MCU Dialog Box"</a> on page 120.
Selected gateways	Lists the selected gateways. The arrow buttons move gateways from one list to the other.

See also:

["Call Server Configuration"](#) on page 203

## Edit Simplified Gateway Dialing Prefix Dialog Box

The **Edit Simplified Gateway Dialing Prefix** dialog box lets you edit a prefix-driven simplified gateway dialing service.

The following table describes the fields in the dialog box.

**Table 10-20** Fields in the Edit Simplified Gateway Dialing Prefix dialog box

Column	Description
Name	A display name for this service.
Description	Brief description of the service.
Enabled	Clearing this check box lets you turn off the service without deleting it.
Simplified dialing prefix	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 <i>Dial services by prefix</i> 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.
Use all gateways	Indicates whether this service applies to all available gateways or only those selected below.
Available gateways	Lists the gateways that have at least one session profile specifying an H.320 or PSTN protocol. See <a href="#">“Edit MCU Dialog Box”</a> on page 120.
Selected gateways	Lists the selected gateways. The arrow buttons move gateways from one list to the other.

See also:

[“Call Server Configuration”](#) on page 203

## 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 an FQDN, rather than an IP address. Then, when there is a failover, the DNS A record for that FQDN can be mapped to a different IP address, changing the Call Server that each endpoint is registered to.

The embedded DNS capability of the Polycom DMA system automates this procedure.



Each Polycom DMA server hosts its own embedded DNS server. It publishes a DNS A record for each site. That A 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.

#### Note

The embedded DNS server publishes only A records, not AAAA records, and thus is not supported in an IPv6 environment.

You can enable these embedded DNS servers on the **Embedded DNS** page. This is a supercluster-wide setting.

If you wish to use this feature, you must also add NS records to your enterprise DNS so that it refers requests to resolve the site-based logical host name to these embedded DNS servers. See [“Additional DNS Records for the Optional Embedded DNS Feature”](#) on page 19.

The following table describes the fields on the **Embedded DNS** page.

**Table 10-21** Fields on the Embedded DNS page

Field	Description
Enable embedded DNS service	Enables the embedded DNS servers.
Call server sub-domain controlled by DMA	FQDN of the logical Call Server domain. For instance: callservers.example.com This is the FQDN for which you must create NS records in your enterprise DNS.

#### To enable DNS publishing

- 1 Be sure you've configured your enterprise DNS with the required NS records (see [“Additional DNS Records for the Optional Embedded DNS Feature”](#) on page 19).
- 2 Go to **Admin > Call Server > Embedded DNS**.
- 3 Click **Enable embedded DNS service**.
- 4 Enter the FQDN for the logical Call Server domain and click **Update**.
- 5 Reconfigure your endpoints to register to the correct FQDN for their site.  
The correct FQDN is:

callserver-*<site name>*.*<FQDN of logical Call Server domain>*

For instance, if the FQDN for the logical Call Server domain is callservers.example.com, the correct FQDN for endpoints in the paris site is:

callserver-paris.callservers.example.com

See also:

[“Call Server Configuration”](#) on page 203

## History Retention Settings

The following table describes the fields on the **History Retention Settings** page. Only users with the Auditor role can access this page.

The settings on this page are supercluster-wide (the clusters aren't independently configured), but the values specified are the number of records to be retained on each cluster, not the total for the entire supercluster.

**Table 10-22** Fields on the History Retention Settings page

Field	Description
Enable recording of registration history	Enables the system to retain Call Server registration records (see <a href="#">“Registration History Report”</a> on page 348).
Registration history records to retain	The number of Call Server registration records to retain on each cluster (up to 500,000).
Signaling message records to retain	The number of Call Server registration signaling records to retain on each cluster (up to 2,000,000).
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.
Call history records to retain	The number of call records to retain on each cluster for retrieval on the Call History page (see <a href="#">“Call History”</a> on page 340).
Conference history records to retain	The number of conference records to retain on each cluster for retrieval on the Conference History page (see <a href="#">“Conference History”</a> on page 341).

**Table 10-22** Fields on the History Retention Settings page (continued)

Field	Description
CDR export history records to retain	The number of records of CDR export operations to retain on each cluster (see <a href="#">“Export History”</a> on page 341).
History record purge interval (seconds)	How often the system checks the registration, call, and conference record levels to see if they exceed the maximums and purges the excess.

**To configure history record retention**

- 1 Log into the system as a user with the Auditor role and go to **Admin > Local Cluster > History Retention Settings**.
- 2 Specify the number of each type of record to retain on each cluster.
- 3 Specify how often you want the system to purge records in excess of those numbers.
- 4 Click **Update**.  
A dialog box informs you that the configuration has been updated.
- 5 Click **OK**.

See also:

[“Call Server Configuration”](#) on page 203



---

# Site Topology

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 site topology configuration topics:

- [About Site Topology](#)
- [Sites](#)
- [Site Links](#)
- [Site-to-Site Exclusions](#)
- [Territories](#)
- [Network Clouds](#)
- [Site Topology Configuration Procedures](#)

## About Site Topology

Site topology information 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 Polycom DMA cluster is responsible. Territories serve multiple purposes in a Polycom DMA system deployment. See [“Territories”](#) on page 257.

The Polycom DMA system uses site topology information for a variety of purposes, including cascading of conferences, bandwidth management, and Session Border Controller selection. It can get it in one of two ways:

- If you have a Polycom CMA system, integrate the Polycom DMA system with it (see [“Polycom CMA System Integration”](#) on page 157) to automatically get its site topology information.

**Note**

Integration with a Polycom CMA system is not supported in **Maximum security** mode.

- If you don't have a Polycom CMA system, enter site topology information about your network directly into the Polycom DMA system's site topology pages.

If your Polycom DMA system is superclustered (see [“About Superclustering”](#) on page 195), site topology data only needs to be created (or obtained from a Polycom CMA system) on one cluster of the supercluster. It's replicated across the supercluster.

For a conference with cascading enabled, the Polycom 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.

When determining which MCU is “nearest” to a caller and which path is best for a cascade link, the system takes into account the bandwidth availability and bit-rate limitations of alternative paths.

**Note**

Cascading always 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. See [“MCU Pool Orders”](#) on page 130.

The cascade links between RMX MCUs must use H.323 signaling. For conferences with cascading enabled, the Polycom 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 Polycom DMA system are also configured for SIP signaling).

See also:

[“Sites”](#) on page 243

[“Site Links”](#) on page 254

[“Site-to-Site Exclusions”](#) on page 256

[“Territories”](#) on page 257

[“Network Clouds”](#) on page 261

[“Site Topology Configuration Procedures”](#) on page 263

## Sites

The **Sites** page contains a list of the sites defined in the site topology.

If the system is integrated with a Polycom CMA system, it receives this information from that system, and this page is read-only. If not, you can enter site information.

The default Internet/VPN site always exists and can't be edited or deleted. It can't be assigned to a territory or controlled by a cluster. Endpoints whose subnet isn't in any other site are considered to be in the Internet/VPN site. They can register to a cluster only if site-less registrations are allowed (see [“Call Server Settings”](#) on page 205).

The commands in the **Actions** list let you add a site, edit or delete sites (other than Internet/VPN), and see information about a site, including the number of devices of each type it contains.

The following table describes the fields in the list.

**Table 11-1** Information in the Sites list

Column	Description
Name	Name of the site.
Description	Description of the site.
Country Code	The country code for the site's location.
Area Code	The city or area code for the site's location.
Max Bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max Bit Rate (kbps)	The per-call bit rate limit for voice and video calls. <b>Note:</b> Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate.
Territory	The territory to which the site belongs, which determines the Polycom DMA cluster responsible for it.

See also:

[“About Site Topology”](#) on page 241

[“Site Information Dialog Box”](#) on page 244

[“Add Site Dialog Box”](#) on page 244

[“Edit Site Dialog Box”](#) on page 248

[“Add Subnet Dialog Box”](#) on page 253

[“Edit Subnet Dialog Box”](#) on page 253

[“Site Topology Configuration Procedures”](#) on page 263

## Site Information Dialog Box

Lets you view information about the selected site, including which subnets are associated with it and counts of the devices it contains.

The following table describes the fields in the dialog box, all of which are read-only.

**Table 11-2** Site Information dialog box

Field	Description
<b>Site Info</b>	
Site name	A meaningful name for the site.
Description	A brief description of the site.
Logical host name	The logical FQDN that endpoints in this site should register to. See <a href="#">“Embedded DNS”</a> on page 236.
<b>Device Types</b>	
MCUs	The number of MCUs in the site.
DMAs	The number of Polycom DMA systems in the site.
VBP	The number of Polycom Video Border Proxy NAT/firewall traversal appliances in the site.
Endpoints	The number of registered endpoints in the site.
<b>Subnets</b>	A list of the subnets in the site.

See also:

[“About Site Topology”](#) on page 241

[“Sites”](#) on page 243

## Add Site Dialog Box

Lets you define a new site in the Polycom DMA system’s site topology and specify which subnets are associated with it. The following table describes the fields in the dialog box.



**Table 11-3** Add Site dialog box

Field	Description
<b>General Info</b>	
<b>General Settings</b>	
Site name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
<b>Bandwidth Settings</b>	
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls. <b>Note:</b> Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate selected.
<b>Territory Settings</b>	
Territory	Assigns the site to a territory, and thus to a Polycom DMA cluster.
<b>ISDN Number Assignment</b>	
Assignment method	<p>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.</p> <p>The assignment options are:</p> <ul style="list-style-type: none"> <li>• <b>No assignment.</b> Select this option when you don't want to define a range of E.164 aliases for the site.</li> <li>• <b>Manual assignment.</b> Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.</li> <li>• <b>Automatic assignment.</b> 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.</li> </ul> <p>After an E.164 alias is assigned to an endpoint, it's reserved for use as long as that endpoint remains registered with the Polycom DMA system.</p> <p>If you decide not to enable <b>Automatic assignment</b>, you can always manually add E.164 aliases to endpoints from the <b>Endpoints</b> page (see <a href="#">“Edit Device Dialog Box”</a> on page 78). And endpoints will have any aliases with which they register.</p>

**Table 11-3** Add Site dialog box (continued)

Field	Description
Dialing method	<p>The ISDN inward dialing method for the site:</p> <ul style="list-style-type: none"> <li>• <b>DID (Direct Inward Dial)</b>. 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.</li> <li>• <b>Gateway Extension Dialing</b>. 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.</li> </ul> <p>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.</p>
<b>ISDN Outbound Dialing</b>	
Override ITU dialing rules	<p>Check this box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway.</p> <p>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.</p>
PBX access code	The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.
Country code	<p>The country code for the site's location. Click the CC button to select from a list of countries.</p> <p>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.</p>
Area code	<p>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.</p> <p>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.</p>
Always dial area code	Specifies that the area code should always be included in the phone number.
Always dial national prefix	Specifies that the national prefix should always be included in the phone number.

**Table 11-3** Add Site dialog box (continued)

Field	Description
Length of subscriber number	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.
<b>ISDN Range Assignment (for DID dialing method)</b>	
Length of call line identifier	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.
Length of short phone number	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.
ISDN Number Ranges	The number ranges available for assignment to endpoints in the site. Click <b>Add</b> to add a new range of numbers. Click <b>Edit</b> or <b>Delete</b> 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.
<b>ISDN Range Assignment (for gateway extension dialing method)</b>	
ISDN gateway number	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.
E.164 start	The beginning of the range of E.164 extensions associated with the site.
E.164 end	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.
<b>H.323 Routing</b>	
Internet calls are not allowed	Disables H.323 calls from the internet.
Allowed via H.323-aware firewall	Allows calls from the internet through a firewall.

**Table 11-3** Add Site dialog box (continued)

Field	Description
Allowed via H.323-aware SBC or ALG	Allows calls from the internet only through a session border controller (SBC) or application layer gateway (ALG).
Call signaling address	The call signaling address for the SBC.
Port	The call signaling port for the SBC.
<b>SIP Routing</b>	
Internet calls are not allowed	Disables SIP calls from the internet.
Allowed via SIP-aware firewall	Allows calls from the internet through a firewall.
Allowed via SIP-aware SBC or ALG	Allows calls from the internet only through a session border controller (SBC) or application layer gateway (ALG).
Call signaling address	The call signaling address for the SBC.
Port	The call signaling port for the SBC.
<b>Subnets</b>	
IP Address	The IP address that defines the subnet.
Subnet Mask	The subnet mask for the site.
Max Bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max Bit Rate (kbps)	The per-call bit rate limit for voice and video calls.

See also:

[“About Site Topology”](#) on page 241

[“Sites”](#) on page 243

[“Add Subnet Dialog Box”](#) on page 253

[“Edit Subnet Dialog Box”](#) on page 253

[“Site Topology Configuration Procedures”](#) on page 263

## Edit Site Dialog Box

Lets you edit a site in the Polycom DMA system’s site topology and add or edit a subnet associated with the site. The following table describes the fields in the dialog box.

**Table 11-4** Edit Site dialog box

Field	Description
<b>General Info</b>	
<b>General Settings</b>	
Site name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
<b>Bandwidth Settings</b>	
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls. <b>Note:</b> Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate selected.
<b>Territory Settings</b>	
Territory	Assigns the site to a territory, and thus to a Polycom DMA cluster.
<b>ISDN Number Assignment</b>	
Assignment method	<p>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.</p> <p>The assignment options are:</p> <ul style="list-style-type: none"> <li>• <b>No assignment.</b> Select this option when you don't want to define a range of E.164 aliases for the site.</li> <li>• <b>Manual assignment.</b> Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints.</li> <li>• <b>Automatic assignment.</b> 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.</li> </ul> <p>After an E.164 alias is assigned to an endpoint, it's reserved for use as long as that endpoint remains registered with the Polycom DMA system.</p> <p>If you decide not to enable <b>Automatic assignment</b>, you can always manually add E.164 aliases to endpoints from the <b>Endpoints</b> page (see <a href="#">"Edit Device Dialog Box"</a> on page 78). And endpoints will have any aliases with which they register.</p>

**Table 11-4** Edit Site dialog box (continued)

Field	Description
Dialing method	<p>The ISDN inward dialing method for the site:</p> <ul style="list-style-type: none"> <li>• <b>DID (Direct Inward Dial)</b>. 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.</li> <li>• <b>Gateway Extension Dialing</b>. 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.</li> </ul> <p>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.</p>
<b>ISDN Outbound Dialing</b>	
Override ITU dialing rules	<p>Check this box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway.</p> <p>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.</p>
PBX access code	The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.
Country code	<p>The country code for the site's location. Click the CC button to select from a list of countries.</p> <p>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.</p>
Area code	<p>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.</p> <p>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.</p>
Always dial area code	Specifies that the area code should always be included in the phone number.

**Table 11-4** Edit Site dialog box (continued)

Field	Description
Always dial national prefix	Specifies that the national prefix should always be included in the phone number.
Length of subscriber number	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.
<b>ISDN Range Assignment (for DID dialing method)</b>	
Length of call line identifier	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.
Length of short phone number	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.
ISDN Number Ranges	The number ranges available for assignment to endpoints in the site. Click <b>Add</b> to add a new range of numbers. Click <b>Edit</b> or <b>Delete</b> 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.
<b>ISDN Range Assignment (for gateway extension dialing method)</b>	
ISDN gateway number	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.
E.164 start	The beginning of the range of E.164 extensions associated with the site.
E.164 end	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.

**Table 11-4** Edit Site dialog box (continued)

Field	Description
<b>H.323 Routing</b>	
Internet calls are not allowed	Disables H.323 calls from the internet.
Allowed via H.323-aware firewall	Enables calls from the internet through a firewall.
Allowed via H.323-aware SBC or ALG	Enables calls from the internet through a session border controller (SBC) or application layer gateway (ALG).
Call signaling address	The call signaling address for the SBC.
Port	The call signaling port for the SBC.
<b>SIP Routing</b>	
Internet calls are not allowed	Disables SIP calls from the internet.
Allowed via SIP-aware firewall	Enables calls from the internet through a firewall.
Allowed via SIP-aware SBC or ALG	Enables calls from the internet through a session border controller (SBC) or application layer gateway (ALG).
Call signaling address	The call signaling address for the SBC.
Port	The call signaling port for the SBC.
<b>Subnets</b>	
IP Address	The IP address that defines the subnet.
Subnet Mask	The subnet mask for the site.
Max Bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max Bit Rate (kbps)	The per-call bit rate limit for voice and video calls.

See also:

[“About Site Topology”](#) on page 241

[“Sites”](#) on page 243

[“Add Subnet Dialog Box”](#) on page 253

[“Edit Subnet Dialog Box”](#) on page 253

[“Site Topology Configuration Procedures”](#) on page 263



## Add Subnet Dialog Box

Lets you add subnets to the site you're adding or editing. The following table describes the fields in the dialog box.

**Table 11-5** *Add Subnet dialog box*

Field	Description
IP address	The IP address that defines the subnet.
Subnet mask	The subnet mask, such as 255.255.255.0.
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls.

### Note

You can assign a subnet to only one site.

See also:

[“Add Site Dialog Box”](#) on page 244

[“Edit Site Dialog Box”](#) on page 248

[“Site Topology Configuration Procedures”](#) on page 263

## Edit Subnet Dialog Box

Lets you edit a subnet associated with a site. The following table describes the fields in the dialog box.

**Table 11-6** *Edit Subnet dialog box*

Field	Description
IP address	The IP address that defines the subnet.
Subnet mask	The subnet mask, such as 255.255.255.0.
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls.

### Note

You can assign a subnet to only one site.

See also:

[“Add Site Dialog Box”](#) on page 244

[“Edit Site Dialog Box”](#) on page 248

[“Site Topology Configuration Procedures”](#) on page 263

## Site Links

The **Site Links** page contains a list of the links defined in the site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see [“Network Clouds”](#) on page 261).

If the system is integrated with a Polycom CMA system, it receives this information from that system, and this page is read-only. If not, you can enter link information.

The commands in the **Actions** list let you add a link and edit or delete existing links.

The following table describes the fields in the list.

**Table 11-7** Information in the Site Links list

Column	Description
Name	Name of the link.
Description	Description of the link.
From Site	The originating site of the link.
To Site	The destination site (or MPLS cloud) of the link.
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls, which you set at the gateway or router.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls, which you set at the gateway or router.

See also:

[“About Site Topology”](#) on page 241

[“Add Site Link Dialog Box”](#) on page 255

[“Edit Site Link Dialog Box”](#) on page 255

[“Site Topology Configuration Procedures”](#) on page 263

## Add Site Link Dialog Box

Lets you define a new site link in thePolycom DMA system’s site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see “[Network Clouds](#)” on page 261).

The following table describes the fields in the dialog box.

**Table 11-8** Add Site Link dialog box

Field	Description
Name	A meaningful name for the link (up to 128 characters).
Description	A brief description of the link (up to 200 characters).
From site	The originating site of the link. Can’t be changed for a site-to-cloud link.
To site	The destination site of the link. Can’t be changed for a site-to-cloud link.
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls, which you set at the gateway or router.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls, which you set at the gateway or router.

See also:

“[About Site Topology](#)” on page 241

“[Site Links](#)” on page 254

“[Site Topology Configuration Procedures](#)” on page 263

## Edit Site Link Dialog Box

Lets you edit a site link in thePolycom DMA system’s site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see “[Network Clouds](#)” on page 261).

The following table describes the fields in the dialog box.

**Table 11-9** Edit Site Link dialog box

Field	Description
Name	A meaningful name for the link (up to 128 characters).
Description	A brief description of the link (up to 200 characters).
From site	The originating site of the link. Can’t be changed for a site-to-cloud link.

**Table 11-9** *Edit Site Link dialog box (continued)*

Field	Description
To site	The destination site of the link. Can't be changed for a site-to-cloud link.
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls, which you set at the gateway or router.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls, which you set at the gateway or router.

See also:

[“About Site Topology”](#) on page 241

[“Site Links”](#) on page 254

[“Site Topology Configuration Procedures”](#) on page 263

## Site-to-Site Exclusions

The **Site-to-Site Exclusions** page contains a list of the site-to-site connections that the site topology doesn't permit a call or session to use.

If the system is integrated with a Polycom CMA system, it receives this information from that system, and this page is read-only. If not, you can define exclusions.

The commands in the **Actions** list let you add a site-to-site exclusion and delete existing exclusions.

The following table describes the fields in the list.

**Table 11-10** *Information in the Site-to-Site Exclusions list*

Column	Description
From/To Site	Name of one of the two sites connected by the excluded link.
To/From Site	Name of the other site.

See also:

[“About Site Topology”](#) on page 241

[“Add Site-to-Site Exclusion Wizard”](#) on page 257

[“Site Topology Configuration Procedures”](#) on page 263

## Add Site-to-Site Exclusion Wizard

Lets you define a new site-to-site exclusion in the Polycom DMA system's site topology.

### To add a site-to-site exclusion

- 1 Go to **Network > 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. Click **Next**.  
If the site you want isn't displayed in the list, you can search by site name or territory.
- 4 In Step 2 of the wizard, select the second site for the exclusion. Click **Next**.
- 5 In Step 3 of the wizard, review the exclusion and click **Done** if it's correct.

See also:

["Site-to-Site Exclusions"](#) on page 256

["Site Topology Configuration Procedures"](#) on page 263

## Territories

The **Territories** page lists the territories defined in the site topology. On the right, it displays information about the selected territory.

A territory contains one or more sites for which a Polycom DMA cluster is responsible. By default, there is one territory named Default DMA Territory. In a superclustered Polycom DMA system deployment, additional territories allow you to assign different territories to different Polycom 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 Polycom 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 Polycom DMA cluster is responsible for connecting to the directory server and retrieving user and group data.
- Microsoft Exchange server integration (for calendaring service) is associated with a territory, thus specifying which Polycom DMA cluster is responsible for integrating with the Exchange server and monitoring the Polycom Conferencing infrastructure mailbox.

- The Polycom DMA system's Conference Manager functionality is associated with territories, thus specifying which Polycom 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 Polycom CMA system, it receives territory information from that system, and the **Territories** page is view-only. If not, you can modify the territory information.

The commands in the **Actions** list let you add a territory and edit or delete territories, or if the system is integrated with a Polycom CMA system, view details for a territory.

The following table describes the fields in the list and the sections on the right.

**Table 11-11** Information on the Territories page

Column/Section	Description
Name	Name of the territory.
Description	Description of the territory.
Primary Cluster	The primary Polycom DMA cluster responsible for this territory.
Backup Cluster	The backup Polycom DMA cluster, if any, responsible for this territory. You must have a supercluster consisting of at least two Polycom DMA clusters in order to specify a backup.
<b>Territory Summary</b> pane	Repeats the name and description of the selected territory.
<b>Associated Sites</b> pane	List the sites included in the selected territory.

See also:

[“About Site Topology”](#) on page 241

[“Add Territory Dialog Box”](#) on page 259

[“Edit Territory Dialog Box”](#) on page 260

[“Site Topology Configuration Procedures”](#) on page 263

## Add Territory Dialog Box

Lets you define a new territory in the Polycom DMA system's site topology. The following table describes the fields in the dialog box.

**Table 11-12** Add Territory dialog box

Field	Description
<b>Territory Info</b>	
Name	A meaningful name for the territory (up to 128 characters).
Description	A brief description of the territory (up to 200 characters).
Primary cluster	The primary Polycom DMA cluster responsible for this territory.
Backup cluster	The backup Polycom DMA cluster, if any, responsible for this territory. You must have a supercluster consisting of at least two Polycom DMA clusters in order to specify a backup.
Host conference rooms in this territory	Enables this territory to be used for hosting conference rooms (VMRs, or virtual meeting rooms). The territory's primary and backup clusters must both be licensed for conference room hosting. No more than three territories may have this capability enabled.
<b>Associated Sites</b>	
Search sites	Enter search string or leave blank to find all sites.
Available sites	Lists sites found and shows the territory, if any, to which each currently belongs. Selecting a site and moving it to the <b>Associated sites</b> list changes its territory assignment to this territory.
Associated sites	Lists sites linked to this territory. Changes you make to this list aren't implemented until you click <b>OK</b> .

See also:

["About Site Topology"](#) on page 241

["Territories"](#) on page 257

["Site Topology Configuration Procedures"](#) on page 263

## Edit Territory Dialog Box

Lets you edit a territory in the Polycom DMA system's site topology.

The following table describes the fields in the dialog box.

**Table 11-13** Edit Territory dialog box

Field	Description
<b>Territory Info</b>	
Name	A meaningful name for the territory (up to 128 characters).
Description	A brief description of the territory (up to 200 characters).
Primary cluster	The primary Polycom DMA cluster responsible for this territory.
Backup cluster	The backup Polycom DMA cluster, if any, responsible for this territory. You must have a supercluster consisting of at least two Polycom DMA clusters in order to specify a backup.
Host conference rooms in this territory	Enables this territory to be used for hosting conference rooms (VMRs, or virtual meeting rooms). The territory's primary and backup clusters must both be licensed for conference room hosting. No more than three territories may have this capability enabled.
<b>Associated Sites</b>	
Search sites	Enter search string or leave blank to find all sites.
Available sites	Lists sites found and shows the territory, if any, to which each currently belongs. Selecting a site and moving it to the <b>Associated sites</b> list changes its territory assignment to this territory.
Associated sites	Lists sites linked to this territory. Changes you make to this list aren't implemented until you click <b>OK</b> .

See also:

["About Site Topology"](#) on page 241

["Territories"](#) on page 257

["Site Topology Configuration Procedures"](#) on page 263



## Network Clouds

The **Network Clouds** page contains a list of the MPLS (Multiprotocol Label Switching) network clouds defined in the site topology.

If the system is integrated with a Polycom CMA system, it receives MPLS network information from that system, and this page is read-only. If not, you can enter MPLS network cloud information.

The commands in the **Actions** list let you add an MPLS cloud and edit or delete existing MPLS clouds.

The following table describes the fields in the list.

**Table 11-14** Information in the Network Clouds list

Column/Section	Description
Name	Name of the cloud.
Description	Description of the cloud.

See also:

[“About Site Topology”](#) on page 241

[“Add Network Cloud Dialog Box”](#) on page 261

[“Edit Network Cloud Dialog Box”](#) on page 262

[“Site Topology Configuration Procedures”](#) on page 263

## Add Network Cloud Dialog Box

Lets you define a new MPLS network cloud in the Polycom DMA system’s site topology. The following table describes the fields in the dialog box.

**Table 11-15** Add Network Cloud dialog box

Field	Description
<b>Cloud Info</b>	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).

**Table 11-15** Add Network Cloud dialog box (continued)

Field	Description
<b>Associated Sites</b>	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each belongs. Select a site and click the right arrow to open the <b>Add Site Link</b> dialog box (see <a href="#">“Add Site Link Dialog Box”</a> on page 255).
Associated Sites	Lists sites linked to the cloud and shows the territory, if any, to which each belongs.

See also:

[“About Site Topology”](#) on page 241

[“Network Clouds”](#) on page 261

[“Site Topology Configuration Procedures”](#) on page 263

## Edit Network Cloud Dialog Box

Lets you edit an MPLS network cloud in thePolycom DMA system’s site topology. The following table describes the fields in the dialog box.

**Table 11-16** Edit Network Cloud dialog box

Field	Description
<b>Cloud Info</b>	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).
<b>Associated Sites</b>	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each belongs. Select a site and click the right arrow to open the <b>Add Site Link</b> dialog box (see <a href="#">“Add Site Link Dialog Box”</a> on page 255).
Associated Sites	Lists sites linked to the cloud and shows the territory, if any, to which each belongs.

See also:

[“About Site Topology”](#) on page 241

[“Network Clouds”](#) on page 261

[“Site Topology Configuration Procedures”](#) on page 263

## Site Topology Configuration Procedures

### To configure your site topology

**1** Go to **Network > Site Topology > Sites**.

Initially, the list of sites contains only an entry named Internet/VPN, which can't be edited.

**2** For each site in your network topology, do the following:

**a** In the **Actions** list, click **Add**.

**b** In the **Add Site** dialog box, complete the **General Info** section. See [“Add Site Dialog Box”](#) on page 244.

**c** To enable IP calls to/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. See [“Add Subnet Dialog Box”](#) on page 253.

**e** Click **OK**.

**3** Go to **Network > Site Topology > Territories**.

The list of territories contains an entry named Default DMA Territory. It's assigned to this Polycom DMA system cluster. You can edit this entry, including changing its name and assigning sites to it.

**4** Edit the Default DMA Territory entry:

**a** Select the entry and, in the **Actions** list, click **Edit**.

The **Edit Territory** dialog box 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. See [“Edit Territory Dialog Box”](#) on page 260.

**d** Click **OK**.

**5** Add other territories by clicking **Add** in the **Actions** list and completing the same settings in the **Add Territory** dialog box.

- 6** Go to **Network > 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 box, define the link. See [“Add Site Link Dialog Box”](#) on page 255.
  - c** Click **OK**.
- 7** Go to **Network > 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 box 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. See [“Add Network Cloud Dialog Box”](#) on page 261.
  - 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 box appears.
  - e** Define the link. See [“Add Site Link Dialog Box”](#) on page 255.
  - f** Repeat the previous two steps for each additional site linked to this cloud.
  - g** Click **OK**.
- 8** Go to **Network > 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. See [“Add Site-to-Site Exclusion Wizard”](#) on page 257.

Your site topology information is complete. For conferences with cascading enabled, the Polycom DMA system can use it 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.

**Note**

If in the future, you integrate this system with a Polycom CMA system, the site topology information from the Polycom CMA system will replace the information you entered.

See also:

[“About Site Topology”](#) on page 241

# Users and Groups

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system management topics related to users and groups:

- [User Roles Overview](#)
- [Adding Users Overview](#)
- [Users](#)
- [Groups](#)
- [Login Sessions](#)
- [Change Password Dialog Box](#)

## User Roles Overview

The Polycom 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 only three of the four roles must be explicitly assigned).

The following table briefly describes the user roles. See [“Polycom DMA System Management Interface Access”](#) on page 6 for detailed information on which commands are available to each user role.

**Table 12-1** The Polycom DMA system's user roles

Role	Description
Administrator	Responsible for the overall administration of the system. Can access all the pages except those reserved for auditors (must be enterprise user to see enterprise reports, enterprise users, and groups). This role must be explicitly assigned by an Administrator.
Auditor	Responsible for configuring logging and history record retention, and for managing logs. Can access all history reports. This role must be explicitly assigned by an Administrator.
Provisioner	Responsible for the management of Conferencing User accounts. Can create or modify only users with no role other than Conferencing User, but can view all local users and, if an enterprise user, all enterprise users. Can view history reports. This role must be explicitly assigned by an Administrator.
Conferencing User	Can use the system's ad hoc conferencing features (and typically has been provisioned with a virtual conference room). Cannot access any system management interfaces. This role is automatically present on all user accounts. It isn't listed under <b>Available Roles</b> or explicitly assigned.

If your system is integrated with an Active Directory, all enterprise users are automatically Conferencing Users. You can use enterprise groups to manage assignment of the other user roles. See [“Enterprise Groups Procedures”](#) on page 287.

#### Note

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.

See also:

[“Adding Users Overview”](#) on page 267

[“Users Procedures”](#) on page 280

[“Conference Rooms Procedures”](#) on page 282

## Adding Users Overview

You can add users to the system in two ways:

- Add users manually to the Polycom DMA system. These are known as *local* users. When adding users manually, you must assign them conference rooms and any specific roles they should have.
- Integrate the Polycom DMA system with Microsoft Active Directory (requires Administrator permissions). This integration allows users with specific roles (Administrator, Auditor, or Provisioner) to log into the Polycom DMA system with their Active Directory user names and passwords.

When a Polycom DMA system is integrated with an Active Directory, the Active Directory users are automatically added as Polycom DMA system users with a Conferencing User role and displayed in the Polycom DMA system **Users** list. An administrator can assign them additional roles as required.

### Note

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.

A newly installed system has a single local user account, admin. We strongly recommend that, as part of initial system setup, you create a local user account for yourself with the Administrator role, log in using that account, and delete the admin user account. See the caution and first procedure in [“Users Procedures”](#) on page 280.

You can then create other local user accounts or integrate with an Active Directory and assign additional roles to the appropriate enterprise users.

Integration with an Active Directory is described in [“Microsoft Active Directory Integration”](#) on page 135.

See also:

[“Polycom® DMA™ System Initial Configuration Summary”](#) on page 17

[“User Roles Overview”](#) on page 265

[“Users Procedures”](#) on page 280

[“Conference Rooms Procedures”](#) on page 282

## Users

The **Users** page provides access to information about both local and enterprise users. From it, you can:

- Add local users.
- Edit both local and enterprise users (for the latter, only roles and conference passcodes can be modified).
- Manage conference rooms (virtual meeting rooms, or VMRs) for both local and enterprise users.

The search pane above the list lets you find users matching the criteria you specify. Click the down arrow on the right to expand the search pane, providing access to more search fields and filters.

The system matches any string you enter against the beginning of the value for which you're searching. For the **Search users** field at the top, it matches against user ID, first name, and last name. For instance, if you enter "sa" in the **Search users** field, it displays the users whose user ID, first name, or last name begins with "sa."

To search for a string not at the beginning of the field, you can use an asterisk (\*) as a wildcard. You can restrict the search to local users by selecting the check box.

The users that match your search criteria are listed below.

The following table describes the parts of the **Users** list.

**Table 12-2** Information in the Users list

Column	Description
User ID	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.
First Name	The user's first name.
Last Name	The user's last name.
Domain	The domain associated with the user. All users added manually to the system are in the LOCAL domain.
Conference Rooms	The user's conference room or rooms (virtual meeting rooms, or 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. 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.



**Table 12-2** Information in the Users list (continued)

Column	Description
Roles	The user's explicitly assigned user roles, if any. All users automatically have the Conferencing User role; it's not listed or explicitly assigned (but a conference room ID is required). See <a href="#">"User Roles Overview"</a> on page 265.
Chairperson Passcode	The numeric passcode that identifies chairpersons in the user's conferences. If none, the user's conferences don't include the chairperson feature.  For enterprise users, passcodes (both kinds) generally come from the Active Directory. See <a href="#">"Adding Passcodes for Enterprise Users"</a> on page 146. But you can specify an enterprise user's passcodes locally. See <a href="#">"Edit User Dialog Box"</a> on page 272.  For local users, you can add passcodes when you create or edit the users. See <a href="#">"Add User Dialog Box"</a> on page 270.
Conference Passcode	The numeric passcodes that callers must enter to join the user's conferences. If none, the user's conferences don't require a passcode.

See also:

["User Roles Overview"](#) on page 265

["Adding Users Overview"](#) on page 267

["Add User Dialog Box"](#) on page 270

["Edit User Dialog Box"](#) on page 272

["Users Procedures"](#) on page 280

["Conference Rooms Procedures"](#) on page 282

## Add User Dialog Box

The following table describes the parts of the **Add User** dialog box, which lets you add local users to the system.

**Table 12-3** Add User dialog box

Field	Description
<b>General Info</b>	
First name	The local user's first name.
Last name	The local user's last name.
User ID	The local user's login name.
Password Confirm password	The local user's system login password (not conference or chairperson passcode). The password must satisfy the local password rules specified for the system (see "Local Password" on page 48).
Account disabled	If checked, user does not have conferencing privileges and can't log into the system management interface.
Conference room territory	The territory to which the user's conference rooms (virtual meeting rooms, or VMRs) are assigned. A conference room's territory assignment determines which DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary). If not selected, the user's conference rooms are assigned as follows (in priority order listed): <ul style="list-style-type: none"> <li>To the territory associated with the room specifically (see "Conference Rooms Dialog Box" on page 275).</li> <li>Otherwise, to the territory associated with the AD group the user belongs to (if more than one, the lexically first group) (see "Edit Group Dialog Box" on page 286).</li> <li>Otherwise, the system's default territory (see "Conference Settings" on page 163).</li> </ul>
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, or if none, the system's default class of service. See "Conference Settings" on page 163.
Maximum bit rate (kbps)	If <b>Class of service</b> is selected, lets you specify the maximum bit rate for the user.

**Table 12-3** Add User dialog box (continued)

Field	Description
Minimum downspeed rate (kbps)	If <b>Class of service</b> is selected, lets you specify the minimum bit rate to which the user's calls can be reduced (downspeeded).
<b>Associated Endpoints</b>	
Associated endpoints	Lists the endpoints associated with the user. Click <b>Select</b> to open the <b>Select Associated Endpoints</b> dialog box and associate an endpoint with the user (see <a href="#">"Select Associated Endpoints Dialog Box"</a> on page 275). Click <b>Delete</b> to delete an associated endpoint. A dialog box prompts you to confirm.  <b>Note:</b> You can also manage endpoint associations on the <b>Endpoints</b> page (see <a href="#">"Associate User Dialog Box"</a> on page 80). But if the Polycom DMA system is integrated with a Polycom CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom CMA system.
<b>Associated Roles</b>	
Available roles	Lists the roles available for assignment to the user. All users automatically have the Conferencing User role; it's not listed or explicitly assigned (but a conference room ID is required). See <a href="#">"User Roles Overview"</a> on page 265.
Selected roles	Lists the roles selected for assignment to the user.
<b>Conference Passcodes</b>	
Chairperson passcode	The numeric passcode that identifies chairpersons in the user's conferences. If none, the user's conferences don't include the chairperson feature.  Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Can't be the same as the conference passcode.
Conference passcode	The numeric passcode that callers must enter to join the user's conferences. If none, the user's conferences don't require a passcode.  Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Can't be the same as the chairperson passcode.

**Note:**

If Cisco (formerly Tandberg) Codian MCUs are included in the Polycom 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.

See also:

["User Roles Overview"](#) on page 265

["Adding Users Overview"](#) on page 267

["Users"](#) on page 268

["Users Procedures"](#) on page 280

["Conference Rooms Procedures"](#) on page 282

## Edit User Dialog Box

The following table describes the parts of the **Edit User** dialog box. The **User ID** is not editable. The other **General Info** items are editable only for local (not enterprise) users.

**Table 12-4** *Edit User dialog box*

Field	Description
<b>General Info</b>	
First name	The user's first name.
Last name	The user's last name.
User ID	The user's login name.
Password Confirm password	The user's system login password (not conference or chairperson passcode). The password must satisfy the local password rules specified for the system (see <a href="#">"Local Password"</a> on page 48).
Account disabled	If checked, user does not have conferencing privileges and can't log into the system management interface.
Account locked	If checked, the system has locked the user's account due to failed login attempts. An administrator can unlock the account by clearing the check box, but can't lock it.

**Table 12-4** Edit User dialog box (continued)

Field	Description
Conference room territory	<p>The territory to which the user's conference rooms (virtual meeting rooms, or VMRs) are assigned.</p> <p>A conference room's territory assignment determines which DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary).</p> <p>If not selected, the user's conference rooms are assigned as follows (in priority order listed):</p> <ul style="list-style-type: none"> <li>To the territory associated with the room specifically (see <a href="#">"Conference Rooms Dialog Box"</a> on page 275).</li> <li>Otherwise, to the territory associated with the AD group the user belongs to (if more than one, the lexically first group) (see <a href="#">"Edit Group Dialog Box"</a> on page 286).</li> <li>Otherwise, the system's default territory (see <a href="#">"Conference Settings"</a> on page 163).</li> </ul>
Class of service	<p>Select to assign the user a class of service, which determines the priority of the user's calls.</p> <p>If not selected, the user receives the highest class of service associated with any group to which the user belongs, or if none, the system's default class of service. See <a href="#">"Conference Settings"</a> on page 163.</p> <p><b>Note:</b> A class of service may also be assigned to an endpoint. See <a href="#">"Endpoints"</a> on page 73.</p>
Maximum bit rate (kbps)	If <b>Class of service</b> is selected, lets you specify the maximum bit rate for the user.
Minimum downspeed rate (kbps)	If <b>Class of service</b> is selected, lets you specify the minimum bit rate to which the user's calls can be reduced (downspeeded).
<b>Associated Endpoints</b>	
Associated endpoints	<p>Lists the endpoints associated with the user. Click <b>Select</b> to open the <b>Select Associated Endpoints</b> dialog box and associate an endpoint with the user (see <a href="#">"Select Associated Endpoints Dialog Box"</a> on page 275).</p> <p>Click <b>Delete</b> to delete an associated endpoint. A dialog box prompts you to confirm.</p> <p><b>Note:</b> You can also manage endpoint associations on the <b>Endpoints</b> page (see <a href="#">"Associate User Dialog Box"</a> on page 80). But if the Polycom DMA system is integrated with a Polycom CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom CMA system.</p>

**Table 12-4** Edit User dialog box (continued)

Field	Description
<b>Associated Roles</b>	
Available roles	Lists the roles available for assignment to the user. All users automatically have the Conferencing User role; it's not listed or explicitly assigned (but a conference room ID is required). See <a href="#">"User Roles Overview"</a> on page 265.
Selected roles	Lists the roles selected for assignment to the user.
<b>Conference Passcodes</b>	
Chairperson passcode	The numeric passcode that identifies chairpersons in the user's conferences. If none, the user's conferences don't include the chairperson feature.  Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Can't be the same as the conference passcode.
Conference passcode	The numeric passcode that callers must enter to join the user's conferences. If none, the user's conferences don't require a passcode.  Must contain numeric characters only (the digits 0-9) and may be up to 16 digits long. Can't be the same as the chairperson passcode.

**Note:**

If Cisco (formerly Tandberg) Codian MCUs are included in the Polycom 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.

See also:

["User Roles Overview"](#) on page 265

["Adding Users Overview"](#) on page 267

["Users"](#) on page 268

["Users Procedures"](#) on page 280

["Conference Rooms Procedures"](#) on page 282

## Select Associated Endpoints Dialog Box

### Note

If the Polycom DMA system is integrated with a Polycom CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom CMA system.

Lets you associate an endpoint with the selected user.

Use the search fields at the top of the dialog box to find the endpoint you want to associate with this user. Select it in the table below and click **OK**. The dialog box closes and the endpoint is added to the user's **Associated endpoints** list.

### Note

You can also manage endpoint associations on the **Endpoints** page (see ["Associate User Dialog Box" on page 80](#)).

See also:

["Add User Dialog Box" on page 270](#)

["Edit User Dialog Box" on page 272](#)

## Conference Rooms Dialog Box

Lets you view, add, edit, and delete the selected user's conference rooms. A user may have three kinds 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 can't delete this conference room, but you can modify it.
- Custom conference rooms manually added using the **Add** command in this dialog box.
- Calendared conference rooms created automatically when the user uses the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conference meetings in Outlook. You can modify some of the settings for these conference rooms, but not the ones set in the meeting invitation.

The following table describes the parts of the **Conference Rooms** dialog box.

**Table 12-5** Conference Rooms dialog box

Field	Description
Room ID	The unique ID of the room. Icons identify enterprise conference rooms and calendared conference rooms.
Dial-in #	Number used to dial into conference room. Automatically set to the <a href="#">dialing prefix</a> plus room ID.
Conference Template	The template used by the conference room, which defines the conference properties (or links to the RMX profile) used for its conferences. See " <a href="#">Conference Templates</a> " on page 165. The template assignment can be made at the conference room level, AD group level, or system default level.
MCU Pool Order	MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. See " <a href="#">MCU Pool Orders</a> " on page 130. The pool order assignment can be made at the conference room level, AD group level, or system default level.
Max Participants	Maximum number of callers allowed to join the conference. <b>Automatic</b> means the MCU's maximum is used.
Territory	The territory to which the conference room is assigned. A conference room's territory assignment determines which 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, the user level, the AD group level, or the system default level.
Initial Start Time	For a conference room created by the system for a calendared meeting, the start time and date of the meeting.
Add	Opens the <b>Add Conference Room</b> dialog box, where you can create a new custom conference room for this user.
Edit	Opens the <b>Edit Conference Room</b> dialog box, where you can modify the selected conference room.
Delete	Deletes the selected conference room. You're prompted to confirm. You can't delete enterprise conference rooms or calendared meeting conference rooms, only custom conference rooms added manually in the Polycom DMA system.



See also:

[“User Roles Overview”](#) on page 265

[“Adding Users Overview”](#) on page 267

[“Users”](#) on page 268

[“Add Conference Room Dialog Box”](#) on page 277

[“Edit Conference Room Dialog Box”](#) on page 279

[“Users Procedures”](#) on page 280

[“Conference Rooms Procedures”](#) on page 282

## Add Conference Room Dialog Box

Lets you create a custom conference room for this 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) in order to offer the user a different conferencing experience (template) or just an alternate (maybe simpler) room ID and dial-in number.

The following table describes the parts of the **Add Conference Room** dialog box.

**Table 12-6** Add Conference Room dialog box

Field	Description
Room ID	The unique ID of the conference room. Click <b>Generate</b> to let the system pick an available ID (from the range set in <a href="#">Conference Settings</a> ).
Dial-in #	Number used to dial into conference room. Automatically set to the <a href="#">dialing prefix</a> plus room ID.
Territory	<p>The territory to which the conference room is assigned. A conference room’s territory assignment determines which DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary).</p> <p>If not selected, the conference room is assigned as follows (in priority order listed):</p> <ul style="list-style-type: none"> <li>• To the territory associated with the user (see <a href="#">“Edit User Dialog Box”</a> on page 272).</li> <li>• Otherwise, to the territory associated with the AD group the user belongs to (if more than one, the lexically first group) (see <a href="#">“Edit Group Dialog Box”</a> on page 286).</li> <li>• Otherwise, the system’s default territory (see <a href="#">“Conference Settings”</a> on page 163).</li> </ul>

**Table 12-6** Add Conference Room dialog box (continued)

Field	Description
Conference template	The template used by the conference room, which defines the conference properties (or links to the RMX profile) used for its conferences. See <a href="#">“Conference Templates”</a> on page 165. If not selected, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system’s default template. See <a href="#">“Conference Settings”</a> on page 163.
MCU pool order	MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. See <a href="#">“MCU Pool Orders”</a> on page 130. If not selected, 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. See <a href="#">“Conference Settings”</a> on page 163.
Max participants	Maximum number of callers allowed to join the conference. <b>Automatic</b> means the MCU’s maximum is used. If not selected, the room uses the system’s default maximum. See <a href="#">“Conference Settings”</a> on page 163.
Conference Duration	Maximum duration of a conference (in hours and minutes) or <b>Unlimited</b> (the maximum in this case depends on the MCU). If not selected, the room uses the longest duration associated with any group to which the user belongs, or if none, the system’s default maximum duration. See <a href="#">“Conference Settings”</a> on page 163.

See also:

[“User Roles Overview”](#) on page 265

[“Adding Users Overview”](#) on page 267

[“Users”](#) on page 268

[“Conference Rooms Dialog Box”](#) on page 275

[“Users Procedures”](#) on page 280

[“Conference Rooms Procedures”](#) on page 282

## Edit Conference Room Dialog Box

Lets you view or modify a conference room's details. The following table describes the parts of the **Edit Conference Room** dialog box.

**Table 12-7** Edit Conference Room dialog box

Field	Description
Room ID	<p>The unique ID of the conference room. Can't be edited for an enterprise conference room or calendared meeting conference room.</p> <p>For a custom conference room, click <b>Generate</b> to let the system pick an available ID (from the range set in <a href="#">Conference Settings</a>).</p>
Dial-in #	<p>Number used to dial into conference room. Automatically set to the <a href="#">dialing prefix</a> plus room ID.</p>
Territory	<p>The territory to which the conference room is assigned.</p> <p>A conference room's territory assignment determines which DMA cluster hosts its conferences (the primary cluster for the territory, or its backup cluster if necessary).</p> <p>If not selected, the conference room is assigned as follows (in priority order listed):</p> <ul style="list-style-type: none"> <li>• To the territory associated with the user (see <a href="#">"Edit User Dialog Box"</a> on page 272).</li> <li>• Otherwise, to the territory associated with the AD group the user belongs to (if more than one, the lexically first group) (see <a href="#">"Edit Group Dialog Box"</a> on page 286).</li> <li>• Otherwise, the system's default territory (see <a href="#">"Conference Settings"</a> on page 163).</li> </ul>
Conference template	<p>The template used by the conference room, which defines the conference properties (or links to the RMX profile) used for its conferences. See <a href="#">"Conference Templates"</a> on page 165.</p> <p>If not selected, the room uses the highest-priority template associated with any group to which the user belongs, or if none, the system's default template. See <a href="#">"Conference Settings"</a> on page 163.</p>
MCU pool order	<p>MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. See <a href="#">"MCU Pool Orders"</a> on page 130.</p> <p>If not selected, 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. See <a href="#">"Conference Settings"</a> on page 163.</p>

**Table 12-7** Edit Conference Room dialog box (continued)

Field	Description
Max participants	Maximum number of callers allowed to join the conference. <b>Automatic</b> means the MCU's maximum is used. If not selected, the room uses the system's default maximum. See <a href="#">"Conference Settings"</a> on page 163.
Conference Duration	Maximum duration of a conference (in hours and minutes) or <b>Unlimited</b> (the maximum in this case depends on the MCU). If not selected, the room uses the longest duration associated with any group to which the user belongs, or if none, the system's default maximum duration. See <a href="#">"Conference Settings"</a> on page 163.
Calendar Event	This section appears only for calendared meeting conference rooms. It shows the following (read-only): <ul style="list-style-type: none"> <li>Start time and date (from meeting invitation).</li> <li>Expiration date. The conference room is deleted from the system after this date.</li> </ul>

See also:

["User Roles Overview"](#) on page 265

["Adding Users Overview"](#) on page 267

["Users"](#) on page 268

["Conference Rooms Dialog Box"](#) on page 275

["Users Procedures"](#) on page 280

["Conference Rooms Procedures"](#) on page 282

## Users Procedures

### Caution

To eliminate a serious security risk, perform the first procedure below as soon as possible after installing your system.

### To remove the default admin account and create a local account for yourself with administrative privileges

- 1 Log in as admin and go to **User > Users**.  
The **Users** page appears.
- 2 Create a local user account for yourself with the Administrator role. See ["To add a local user"](#) on page 281.
- 3 Log out and log back in using your new local account.

- 4 Go to **Users > Users** and delete the admin account. See [“To delete a local user”](#) on page 282.

### To find a user or users

- 1 Go to **User > Users**.

The **Users** page appears.

- 2 For a simple search, enter a search string in the **Search users** field and press **ENTER**.

The system matches the string you enter against the beginning of the user ID, first name, and last name. If you enter “sa” it displays users whose IDs or first or last names begin with “sa.” To search for a string not at the beginning of the field, you can use an asterisk (\*) as a wildcard. You can restrict the search to local users by selecting the check box.

- 3 For more search options, click the down arrow to the right.

Additional controls appear that let you search specific fields and use specific filters.

- 4 Select the filters you want, enter search strings for one or more fields, and click **Search**.

The system displays the users matching your search criteria.

### To add a local user

- 1 Go to **User > Users**.

- 2 In the **Actions** list, click **Add**.

- 3 In the **Add User** dialog box, complete the **General Info** fields. See [“Add User Dialog Box”](#) on page 270.

- 4 To assign the user additional roles (besides Conferencing User), click **Roles**. Select the role or roles you want to assign and use the arrow button to move them to the **Selected Roles** list.

- 5 Click **OK**.

### To edit a user

- 1 Go to **User > Users**.

- 2 If necessary, filter the **Users** list to find the user to be modified.

- 3 Select the user and click **Edit**.

- 4 As required, edit the **General Info**, **Roles**, and **Conference Passcodes** sections of the **User Properties** dialog box. See [“Edit User Dialog Box”](#) on page 272.

For enterprise users, you can change their roles and their chairperson and conference passcodes, and you can enable or disable their accounts, but you can't change user names, user IDs, or user passwords. For local users, you can change everything but the user ID.

- 5 Click **OK**.

#### To delete a local user

- 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 and click **Delete User**.
- 4 In the **Delete User** dialog box, click **Yes**.

The user is deleted from the Polycom DMA system.

See also:

[“User Roles Overview”](#) on page 265

[“Adding Users Overview”](#) on page 267

[“Users”](#) on page 268

[“Add User Dialog Box”](#) on page 270

[“Edit User Dialog Box”](#) on page 272

[“Conference Rooms Procedures”](#) on page 282

## Conference Rooms Procedures

#### To add a conference room to a user

- 1 Go to **User > Users** and select the user to whom you want to add a room.
- 2 In the **Actions** list, click **Manage Conf Rooms**.  
The **Conference Rooms** dialog box appears.
- 3 Click **Add**.  
The **Add Conference Room** dialog box appears.
- 4 Complete the settings for the new conference room. See [“Add Conference Room Dialog Box”](#) on page 277.
- 5 Click **OK**.

**To edit one of a user's conference rooms**

- 1** Go to **User > Users** and select the user whose conference room you want to edit.
- 2** In the **Actions** list, click **Manage Conf Rooms**.  
The **Conference Rooms** dialog box appears.
- 3** Select the conference room you want to edit and click **Edit**.  
The **Edit Conference Room** dialog box appears.
- 4** Modify the settings you want to change. See ["Edit Conference Room Dialog Box"](#) on page 279.
- 5** Click **OK**.

**To delete one of a user's custom conference rooms**

- 1** Go to **User > Users** and select the user whose custom conference room you want to delete.
- 2** In the **Actions** list, click **Manage Conf Rooms**.  
The **Conference Rooms** dialog box appears.
- 3** Select the conference room you want to remove and click **Delete**.  
You can't delete an enterprise conference room or a conference room created by the system for a calendared meeting.
- 4** When prompted to confirm, click **Yes**.

See also:

["User Roles Overview"](#) on page 265

["Adding Users Overview"](#) on page 267

["Users"](#) on page 268

["Conference Rooms Dialog Box"](#) on page 275

["Add Conference Room Dialog Box"](#) on page 277

["Edit Conference Room Dialog Box"](#) on page 279

["Users Procedures"](#) on page 280

## Groups

Groups functionality is available only if your Polycom DMA system is integrated with an Active Directory. User groups are defined in your Active Directory and imported into the Polycom DMA system from there.

### Note

- 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 Polycom DMA system supports only security groups (not distribution groups) with universal or global scope.

The **Groups** page provides access to information about enterprise groups. From it, you can:

- Import enterprise groups.
- Specify Polycom DMA system roles to be assigned to members of a group.
- Specify a conference template and MCU pool order to be used for a group.

The following table describes the fields on the **Groups** page.

**Table 12-8** *Fields on the Groups page*

Field	Description
Group Name	Name of the group, as defined in the Active Directory.
Description	Description from the Active Directory.
Domain	Name of the domain to which the group belongs.
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. See <a href="#">"Conference Settings"</a> on page 163.
Conference Template	Template assigned to the group, if any, which defines the conference properties (or links to the RMX profile) used for its conferences. See <a href="#">"Conference Templates"</a> on page 165.  The template assignment can be made at the conference room level, AD group level, or system default level.
MCU Pool Order	MCU pool order assigned to this group, if any, which is used to determine which MCU hosts a conference. See <a href="#">"MCU Pool Orders"</a> on page 130.  The pool order assignment can be made at the room level, group level, or system default level.



**Table 12-8** *Fields on the Groups page (continued)*

Field	Description
Territory	Territory to which the group's conference rooms (virtual meeting rooms, or VMRs) are assigned.  A conference room's territory assignment determines which 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, the user level, the AD group level, or the system default level.
Assigned Roles	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). See <a href="#">"User Roles Overview"</a> on page 265.

See also:

["Users"](#) on page 268

["Import Enterprise Groups Dialog Box"](#) on page 285

["Edit Group Dialog Box"](#) on page 286

["Enterprise Groups Procedures"](#) on page 287

## Import Enterprise Groups Dialog Box

The following table describes the fields in the **Import Enterprise Groups** dialog box.

**Table 12-9** *Fields in the Import Enterprise Groups dialog box*

Field	Description
Search domain	Optionally, select a domain to search.
Group	To find all groups, leave blank. To find groups beginning with a specific letter or letters, enter the string. Then click <b>Search</b> .  You can use a wildcard (*) for more complex searches, such as: <ul style="list-style-type: none"> <li>s*admins</li> <li>*eng*</li> </ul>

**Table 12-9** *Fields in the Import Enterprise Groups dialog box (continued)*

Field	Description
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 <b>Search results</b> box.

See also:

[“Users”](#) on page 268

[“Groups”](#) on page 284

[“Edit Group Dialog Box”](#) on page 286

[“Enterprise Groups Procedures”](#) on page 287

## Edit Group Dialog Box

The following table describes the fields in the **Edit Group** dialog box.

**Table 12-10** *Fields in the Edit Group dialog box*

Field	Description
Class of service	Select to assign the group a class of service other than the system's default (see <a href="#">“Conference Settings”</a> on page 163).
Maximum bit rate (kbps)	If <b>Class of service</b> is selected, specifies the maximum bit rate for the group.
Minimum downspeed bit rate (kbps)	If <b>Class of service</b> is selected, specifies the minimum bit rate to which the group's calls can be reduced (downspeeded).
Conference template	Select to assign a template other than the system's default (see <a href="#">“Conference Settings”</a> on page 163).
MCU pool order	Select to assign the group an MCU pool order other than the system's default (see <a href="#">“Conference Settings”</a> on page 163). See <a href="#">“MCU Pool Orders”</a> on page 130.
Territory	Select to assign the group's conference rooms to a territory other than the system's default (see <a href="#">“Conference Settings”</a> on page 163).

**Table 12-10** Fields in the Edit Group dialog box (continued)

Field	Description
Conference Duration	Select to specify a maximum conference duration other than the system's default (see <a href="#">"Conference Settings"</a> on page 163). If you select <b>Unlimited</b> , the maximum depends on the MCU.
Available roles	Lists the Polycom 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). See <a href="#">"User Roles Overview"</a> on page 265.  Use the arrows to move roles from the <b>Available roles</b> box to the <b>Selected roles</b> 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.

See also:

["Users"](#) on page 268

["Groups"](#) on page 284

["Import Enterprise Groups Dialog Box"](#) on page 285

["Enterprise Groups Procedures"](#) on page 287

## Enterprise Groups Procedures

The Polycom DMA system's ability to import an enterprise group and assign it a conference template lets you customize the conferencing experience for all members of the group.

The ability to assign defined Polycom DMA user roles to an enterprise group lets you manage administrative access to the Polycom DMA system in your Active Directory.

You must be logged into the system as an enterprise user with the Administrator role to perform these procedures.

**To set up an enterprise group for Polycom DMA management and operations users**

- 1 In your Active Directory, create a security group containing the users to whom you want to give access to the Polycom DMA system's management and operations interface.  
  
It's up to you whether you want to assign all the user roles to a single group or create separate groups for each user role.
- 2 On the Polycom DMA system, go to **User > Groups**.
- 3 In the **Actions** list, click **Import Enterprise Groups**.
- 4 In the **Import Enterprise Groups** dialog box, use **Search** to find the system administration group you created. Then move it to the **Groups to import** box and click **OK**. See ["Import Enterprise Groups Dialog Box"](#) on page 285.
- 5 On the **Groups** page, select your new group and, in the **Actions** list, click **Edit**.
- 6 In the **Edit Group** dialog box, move the user roles you want to give members of this group to the **Selected roles** box. See ["Edit Group Dialog Box"](#) on page 286.
- 7 Click **OK**.  
  
All members of this group will now share the system access privileges you assigned to the group.
- 8 To grant Polycom DMA system access privileges to a user or remove those privileges, just add or remove the user from the appropriate enterprise group.

**To specify which MCUs a group uses by assigning an MCU Pool Order**

- 1 If necessary, create the MCU pool and the pool order needed. See ["MCU Pool Procedures"](#) on page 129 and ["MCU Pool Order Procedures"](#) on page 133.
- 2 Go to **User > Groups**, select the group to which you need to assign a pool order, and in the **Actions** list, click **Edit**.
- 3 In the **Edit Group** dialog box's **MCU pool order** list, select the pool order to be used for this group. See ["Edit Group Dialog Box"](#) on page 286.
- 4 Click **OK**.

**To set up a custom conferencing experience for an enterprise group**

- 1 Go to **Admin > Conference Manager > Conference Templates** and create a template that defines the conferencing experience for this group. See ["Conference Templates Procedures"](#) on page 188.

- 2 Optionally, in the **Actions** list, 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 end up using a higher-ranking template.

- 3 Go to **User > Groups**, select the group for which you created the template, and in the **Actions** list, click **Edit**.
- 4 In the **Edit Group** dialog box's **Conference template** list, select the template you created for this group. See ["Edit Group Dialog Box"](#) on page 286.
- 5 Click **OK**.

See also:

["Users"](#) on page 268

["Groups"](#) on page 284

["Import Enterprise Groups Dialog Box"](#) on page 285

["Edit Group Dialog Box"](#) on page 286

## Login Sessions

The **Login Sessions** page displays information about the currently active user login sessions and enables you to terminate a login session. You must be an Administrator user to terminate a login session.

### Note

Session termination is not supported in **Maximum security** mode.

The following table describes the parts of the **Login Sessions** list.

**Table 12-11** Information in the Sessions list

Column	Description
Domain	The domain to which the user belongs.
User ID	The user's login name.
Host Address	The IP address from which the user logged in.
Node Name	The Polycom DMA system node on which the user logged in.
Creation Time	The time and date when the user logged in.

**To terminate a user's login session**

- 1 In the **Login Sessions** list, select the login session you want to terminate.
- 2 In the **Actions** list, click **Terminate Session**.

A dialog box asks you to confirm.

- 3 Click **Yes**.

The system terminates the session immediately. The terminated user is informed that the connection to the server was lost.

See also:

[“Session”](#) on page 49

[“Users and Groups”](#) on page 265

## Change Password Dialog Box

The system may be configured to expire local user passwords after a certain number of days (see [“Local Password”](#) on page 48). If your password has expired when you try to log into the system, the **Change Password** dialog box prompts you for a new password.

You can change your password at other times by going to **User > Change Passwords** (but not more often than specified on the **Local Password** page).

The following table describes the fields in the dialog box.

**Table 12-12** *Change Password dialog box*

Field	Description
User ID	The user name with which you're logging in. Display only.
Old password	For security reasons, you must re-enter your old password.
New password	Enter a new password. The password must satisfy the local password rules specified for the system (see <a href="#">“Local Password”</a> on page 48).
Confirm new password	Retype the password to confirm that you entered it correctly.

See also:

[“Security Settings”](#) on page 41

[“Users and Groups”](#) on page 265

---

# System Management and Maintenance

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system operations topics:

- [Management and Maintenance Overview](#)
- [Recommended Regular Maintenance](#)
- [Dashboard](#)
- [Alerts](#)
- [System Log Files](#)
- [Troubleshooting Utilities](#)
- [Backing Up and Restoring](#)
- [Upgrading the Software](#)
- [Adding a Second Server](#)
- [Replacing a Failed Server](#)
- [Shutting Down and Restarting](#)

## Management and Maintenance Overview

The Polycom DMA system requires relatively little 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. See the appropriate topic for your user role:

- [Administrator Responsibilities](#)
- [Auditor Responsibilities](#)

## Administrator Responsibilities

As a Polycom DMA system administrator, you're 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 MCUs are added. See [“Licenses”](#) on page 59.
- Monitoring system health and performing the recommended regular maintenance. See [“Recommended Regular Maintenance”](#) on page 293.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See [“Troubleshooting Utilities”](#) on page 322. Should the need arise, Polycom Global Services personnel may ask you to run these tools.
- Upgrading the system when upgrades/patches are made available. See [“Upgrading the Software”](#) on page 328.

## Administrative 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, 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 at least one DNS server in your network configuration (see [“Network Settings”](#) on page 54), and preferably two or more. This allows the Polycom DMA system to function properly in the event of a single external DNS failure.
- Configure at least one NTP server in your time configuration (see [“Time Settings”](#) on page 58) and preferably two or more. 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.



- Unless otherwise instructed by Polycom Global Services or to change the default root password after installation, always use the **High Security** setting. See [“Security Settings”](#) on page 41.

## Auditor Responsibilities

As a Polycom 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. See [“Logging Settings”](#) on page 63. These settings affect the number and the contents of the log archives available for download from the system. See [“System Log Files”](#) on page 319. 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. See [“History Retention Settings”](#) on page 238. These settings affect how much system activity history is retained on the system and available for download as CDRs. See [“Call History”](#) on page 340, [“Conference History”](#) on page 341, and [“Call Detail Records \(CDRs\)”](#) on page 344.

## 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 production level with a rolling frequency of every day 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 offsite as well as onsite).
- Export CDRs regularly and back them up securely (preferably offsite as well as onsite).

## Recommended Regular Maintenance

Perform the following tasks to keep your Polycom DMA system operating trouble-free and at peak efficiency. These tasks can be done quickly and should be run at least weekly.

### Regular archive of backups

Log into the Polycom DMA system, go to **Maintenance > Backup and Restore**, and check for new backups. If there are new backups, download and archive the latest one.

Every night, the Polycom DMA system determines whether its configuration or database data have changed since the last time it performed a backup. If so, it creates a new backup instance. For details on backups, see [“Backing Up and Restoring”](#) on page 323.

### General system health and capacity checks

On the **Dashboard** (see [“Dashboard”](#) on page 296), verify that:

- There are no alerts indicating problems with any part of the system.
- The **Supercluster Status** pane shows the correct number of servers and clusters, and the network interfaces that should be working (depending on your IP type and split network settings) are up (green up arrow) and in full duplex mode, with the speed correct for your enterprise network.
- The **Territories Status** pane shows that all territories have the correct capabilities, are being managed by their primary cluster, and (if your deployment is so configured), have a backup cluster.

Go to **Reports > Network Usage** (see [“Network Usage Report”](#) on page 358) and view the graph for each cluster with the following capacity-related metrics selected:

- **Call Counts** – If the number of concurrent calls approaches the license limit, you may need to rebalance territory responsibilities, add licensed capacity, or add another cluster.
- **Conference Manager Calls** – If the number of concurrent calls approaches the number of MCU ports available, you may need to add MCU capacity.

View the graph for each site, site link, and subnet with **Calls Dropped** and **Calls Downspeeded** selected. These metrics show only calls dropped or downspeeded due to insufficient bandwidth at the selected throttlepoint. Any values above zero are indicators of bandwidth saturation and suggest that it's time to increase network bandwidth.

### Microsoft Active Directory health

If the Polycom DMA system is integrated with an Active Directory, check the following (you must be logged in as an enterprise user):

- **Reports > Microsoft Active Directory Integration** (see [“Active Directory Integration Report”](#) on page 349). Check the status and results of the last cache update, and verify that membership information for imported groups, if any, was successfully loaded.
- **Reports > Conference Room Errors** (see [“Conference Room Errors Report”](#) on page 353). 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 Polycom DMA system. They're listed below. Contact your Active Directory administrator to resolve issues with these users.
- **Reports > Orphaned Groups and Users** (see [“Orphaned Groups and Users Report”](#) on page 352). Verify that the number of orphans is not unexpectedly large.
- **Reports > Enterprise Passcode Errors** (see [“Enterprise Passcode Errors Report”](#) on page 355). If you're assigning conference and/or chairperson passcodes to enterprise users, verify that the number of passcode errors is not unexpectedly large.

### Security configuration

Go to **Admin > Local Cluster > Security Settings** and verify that the security settings are what you expect (we strongly recommend always using the high security mode). Any departure from the settings you expected to see may indicate that your system has been compromised. See [“Security Settings”](#) on page 41.

### Certificates

Go to **Admin > Local Cluster > Certificates** and verify that the list of certificates contains the certificates you've installed and looks as you would expect (an archived screen capture may be helpful for comparison).

Display the details for any certificate you've installed and verify they are as expected (again, an archived screen capture may be helpful for comparison).

### Network usage data export


The 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, so it's very predictable. 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.

Determine an appropriate download interval for your site topology and download network usage data to your PC at that interval. See [“Exporting Network Usage Data”](#) on page 358.

### CDR export

If you want to preserve detailed call and conference history data in spreadsheet form off the Polycom DMA system, periodically download the system's CDR (call detail record) data to your PC. See [“Call Detail Records \(CDRs\)”](#) on page 344.

# Dashboard

When you log into the Polycom DMA system, the system **Dashboard** appears. You can return to the **Dashboard** from any other page by clicking the  (“home”) button to the left of the menus. Use the system **Dashboard** to view information about system health and activity levels.

The **Dashboard** is highly customizable. Initially, it contains six default panes. You can close any of these that you don’t want, and you can add others. You can add multiple copies of the same pane, each showing information for a different cluster.

Click the **Add Panes** button to see the panes that are available. In the **Settings** dialog box (see “[Settings Dialog Box](#)” on page 5), you can specify the maximum number of columns for the **Dashboard**. The panes arrange themselves, up to that number across, to best fit your browser window.

The system remembers your **Dashboard** configuration, and you’ll see the same configuration when you log into any cluster of the supercluster.

The buttons on the right side of each pane’s title bar let you access help, go 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.

An alert icon appears in the title bar of a pane if there is an alert related to its information. Hover over it to see the alert message.

See also:

[“Active Directory Integration Pane”](#) on page 297

[“Call Server Active Calls Pane”](#) on page 297

[“Call Server Registrations Pane”](#) on page 297

[“Cluster Info Pane”](#) on page 298

[“Conference History – Max Participants Pane”](#) on page 298

[“Conference Manager MCUs Pane”](#) on page 298

[“Conference Manager Usage Pane”](#) on page 299

[“Exchange Server Integration Pane”](#) on page 299

[“License Status Pane”](#) on page 300

[“Polycom CMA System Integration Pane”](#) on page 300

[“Supercluster Status Pane”](#) on page 301

[“Territory Status Pane”](#) on page 301

[“User Login History Pane”](#) on page 301

## 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.

Click the **Link** button to go to the **Microsoft Active Directory** page.

See also:

[“Dashboard”](#) on page 296

## Call Server Active Calls Pane

Displays the current number of calls in total and for each cluster of the supercluster and the licensed call limit in total and for each cluster.

In a superclustered environment, a call may span multiple clusters. Such a call is counted on each cluster it spans. The total for all clusters includes these multiple counts of cluster-spanning calls.

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

Click a column heading to sort on that column. Click the **Link** button to go to the **Active Calls** page.

See also:

[“Dashboard”](#) on page 296

## 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.

Click a column heading to sort on that column. Click the **Link** button to go to the **Endpoints** page.

See also:

[“Dashboard”](#) on page 296

## Cluster Info 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 time and uptime
- Server, Proxias, and application software version numbers
- Hardware model and serial number
- Time source
- Management network MAC and IP addresses
- Signaling network MAC and IP addresses (if configured for split network)
- CPU utilization
- Memory usage (hover over the bar chart to see details)
- Swap space (total and free)
- Disk space usage (actual and percentage)
- Log space usage (actual and percentage) and next scheduled log purge

Click the **Link** button to go to the **Logging Settings** page.

See also:

[“Dashboard”](#) on page 296

## 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. You can show the data for all Conference Manager clusters or a specific cluster.

Click the **Link** button to go to the **Conference History** page.

See also:

[“Dashboard”](#) on page 296

## Conference Manager MCUs Pane

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

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

Hover over an icon to see an explanation of it. Click a column heading to sort on that column. Click the **Link** button to go to the **MCUs** page, or click an MCU name to go to the **MCUs** page with that MCU selected.

See also:

[“Dashboard”](#) on page 296

## Conference Manager Usage Pane

Displays usage information for 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.

See also:

[“Dashboard”](#) on page 296

## Exchange Server Integration Pane

If the Polycom DMA system is integrated with a Microsoft Exchange server (see [“Microsoft Exchange Server Integration”](#) on page 153), displays the following:

- The integration status, which can be one of the following:
  - **Unavailable** – A service status or inter-node 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 Polycom DMA system isn’t in the system’s Active Directory cache.
  - **Subscription pending** – The Polycom 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 DMA system’s FQDN).
  - **Exchange authentication failed** – The credentials for the Polycom DMA system’s mailbox are no longer valid (e.g., the password has expired).

- **OK** – The Polycom DMA system is receiving and processing Polycom Conferencing meeting notifications from the Exchange server.
- The host name or IP address for the Exchange server as entered on the **Microsoft Exchange Server** page.
- The Polycom DMA system's mailbox address.
- The number of Polycom Conferencing meetings today.

Click the **Link** button to go to the **Microsoft Exchange Server** page.

See also:

["Dashboard"](#) on page 296

## License Status Pane

Displays the license status of the selected cluster and the number of licensed and active calls.

Click the **Link** button to go to the **Licenses** page (only available if the selected cluster is the one on which you're logged in).

See also:

["Dashboard"](#) on page 296

## Polycom CMA System Integration Pane

If the Polycom DMA system is integrated with a Polycom CMA system (see ["Polycom CMA System Integration"](#) on page 157), displays the following:

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

Click the **Link** button to go to the **Polycom CMA System** page.

See also:

["Dashboard"](#) on page 296



## 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 its out of service (no cluster is managing it). Hover over a name or icon to see details.

Click the **Link** button to go to the **DMAs** page.

See also:

["Dashboard"](#) on page 296

## Territory Status Pane

Lists each territory, its capabilities, and the primary and backup cluster responsible for it. The clusters are color-coded:

- Light green: The cluster is primary for the territory and in service.
- Gray: The cluster is not in service or it's the backup cluster and the primary is in service.
- Dark green: The cluster is busied out.
- Red: The cluster is not connected.
- Yellow: The cluster is the backup cluster for the territory, it's in service, and the primary cluster is not in service.

Hover over a cluster name to see more details. Hover over a capabilities icon to see an explanation of it. Click a column heading to sort on that column. Click the **Link** button to go to the **Territories** page.

See also:

["Dashboard"](#) on page 296

## User Login History Pane

Displays the following information about logins by your user ID:

- The server you're currently logged into.
- The time, date, server logged into, 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.

See also:

["Dashboard"](#) on page 296

## Alerts

On various pages and dashboard panes, the alert icon is used to indicate 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 (that is, that you haven't 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 for investigating the issue. A Help button to the right of the alert description displays the help topic for that alert, which contains additional information about the causes and recommendations for dealing with the alert.

The following sections describe the alerts.

### Alert 1001

**Cluster <cluster> is busied out as of YYYY-MM-DD HH:MM GMT+/-H[:MM].**

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 doesn't 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.

See also:

["Alerts"](#) on page 302

### Alert 1002

**Cluster <cluster> is out of service as of YYYY-MM-DD HH:MM GMT+/-H[:MM].**

You or another administrator took the cluster out of service (or busied out the cluster, and now all calls and conferences have ended).

An out-of-service cluster is still running and accessible via the management interface, but doesn't accept any calls or registrations.

Click the link to go to the **DMAs** page.

See also:

["Alerts"](#) on page 302

## Alert 1003

### **Cluster <cluster> is orphaned.**

The replication link with the specified cluster seems to be corrupted.

Click the link to go to the **DMAs** page. Try removing that cluster from the supercluster and then rejoining.

See also:

[“Alerts”](#) on page 302

## Alert 1004

### **Cluster <cluster> is not reachable. Last heartbeat received YYYY-MM-DD HH:MM GMT+/-H[:MM].**

The specified cluster is no longer communicating with the supercluster. The server(s) may be offline or rebooting, or there may be a network problem.

Click the link to go to the **DMAs** page.

See also:

[“Alerts”](#) on page 302

## Alert 1101

### **Territory <territory> not active; Both primary cluster <p-cluster> and backup cluster <b-cluster> not in service.**

The territory’s primary and backup cluster are both unreachable.

This may indicate serious network problems. It’s 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.

See also:

[“Alerts”](#) on page 302

## Alert 1102

### **Territory <territory> not active; cluster <cluster> not in service.**

The territory’s primary cluster is unreachable and it has no backup 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 **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.

See also:

[“Alerts”](#) on page 302

## Alert 1103

### **No clusters assigned to <list of territories>.**

The specified territory or territories are not assigned to a cluster, so any responsibilities assigned to the territories are not being fulfilled.

Click the link to go to the **Territories** page. Assign a primary and backup cluster for every territory in your site topology.

See also:

[“Alerts”](#) on page 302

## Alert 1104

### **Territory <territory> primary cluster <clustername> not in service. Territory operating on backup cluster <clustername>.**

The territory’s primary cluster is unreachable, and its backup cluster has taken over.

This may indicate a network problem. It’s 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-node cluster, and you can’t ping either the virtual or physical IP addresses, look for a network problem. It’s unlikely that both nodes 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 server(s).

See also:

[“Alerts”](#) on page 302

## Alert 2001

**<formatted string from server>**

An error occurred when the cluster responsible for CMA integration tried to synchronized data with the Polycom CMA system. The alert text describes the nature of the problem, which may require remedial action on the Polycom CMA system.

See also:

[“Alerts”](#) on page 302

## Alert 2002

**CMA System <cmaserver> unreachable. Last contact on: YYYY-MM-DD HH:MM GMT+/-H[:MM].**

The cluster responsible for CMA integration was unable to connect to the Polycom CMA system.

This may indicate a network problem or a problem with the Polycom CMA system.

Try logging into the Polycom CMA system. If you can do so, make sure the login credentials that the DMA system uses to connect to it are still valid.

See also:

[“Alerts”](#) on page 302

## Alert 2101

**Active Directory integration was not successful on cluster <cluster>.**

The cluster responsible for Active Directory integration was unable to update the cache of user and group data.

This may indicate a network problem or a problem with the AD.

If the cluster was unable to log into 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.

See also:

[“Alerts”](#) on page 302

## Alert 2102

### **Zero enterprise conference rooms exist on cluster <cluster>.**

The cluster responsible for Active Directory integration successfully retrieved user and group data, but no conference rooms were generated.

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.

See also:

[“Alerts”](#) on page 302

## Alert 2103

### **Active Directory primary caching cluster <p-cluster> is not in service. Caching by backup cluster <b-cluster>.**

The primary cluster for the territory responsible for Active Directory integration is unreachable, and its backup cluster has taken over responsibility for the caching of AD data.

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. Determine whether the cluster was deliberately shut down. If not, try pinging the cluster’s IP addresses.

If this is a two-node cluster, and you can’t ping either the virtual or physical IP addresses, look for a network problem. It’s unlikely that both nodes 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 server(s).

See also:

[“Alerts”](#) on page 302

## Alert 2104

### **Active Directory service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not in service.**

The primary and backup cluster for the territory responsible for Active Directory integration are both unreachable.

This may indicate serious network problems. It's 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).

See also:

[“Alerts”](#) on page 302

## Alert 2105

### **Active Directory service is not available. Cluster <p-cluster> is not in service.**

The primary cluster for the territory responsible for Active Directory integration is unreachable, and it has no backup 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.

We recommend assigning a backup cluster for each territory.

See also:

[“Alerts”](#) on page 302

## Alert 2106

### **Failed connection from <server> to Active Directory for user authentications at YYYY-MM-DD HH:MM GMT+/-H[:MM].**

The specified cluster tried to connect to the Active Directory in order to authenticate a user's credentials and was unable to do so. 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 into the AD server.

Click the link to go to the **Microsoft Active Directory** page. Make sure the login credentials that the DMA system uses to connect to Active Directory are still valid and update them if necessary.

See also:

[“Alerts”](#) on page 302

## Alert 2107

**Failed connection from <cluster> to Active Directory for caching at YYYY-MM-DD HH:MM GMT+/-H[:MM].**

The cluster responsible for Active Directory integration was unable to log into the AD server.

Click the link to go to the **Microsoft Active Directory** page.

See also:

[“Alerts”](#) on page 302

## Alert 2201

**Calendaring primary integration cluster <p-cluster> is not in service. Integration by backup cluster <b-cluster>.**

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.

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.

See also:

[“Alerts”](#) on page 302

## Alert 2202

**Calendaring service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not in service.**

The primary and backup clusters for the territory responsible for Exchange server integration are both unreachable.

This may indicate serious network problems. It’s 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.

See also:

[“Alerts”](#) on page 302



## Alert 2203

### **Calendaring service is not available. Cluster <p-cluster> is not in service**

The primary cluster for the territory responsible for Exchange server integration is unreachable, and it has no backup 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.

See also:

[“Alerts”](#) on page 302

## Alert 3001

### **No signaling interface enabled for cluster <cluster>. SIP or H.323 must be configured to allow calls.**

The specified cluster has neither H.323 or SIP signaling enabled and is unable to accept calls.

To use the cluster for anything other than logging into the management interface, you must enable signaling.

If you're logged into that cluster, click the link to go to the **Signaling Settings** page. If not, log into that cluster and go to **Admin > Local Cluster > Signaling Settings**.

See also:

[“Alerts”](#) on page 302

## Alert 3101

### **Cluster <cluster>: The server certificate has expired.**

The specified cluster's 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're logged into that cluster, click the link to go to the **Certificates** page. If not, log into that cluster (your browser will warn you not to do this, and you'll have to override its advice) and go to **Admin > Local Cluster > Certificates**.

See also:

[“Alerts”](#) on page 302

## Alert 3102

**Cluster <cluster>: The server certificate will expire within 1 day. All system access may be lost.**

The specified cluster's server certificate is about to expire. 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're logged into that cluster, click the link to go to the **Certificates** page. If not, log into that cluster and go to **Admin > Local Cluster > Certificates**.

See also:

["Alerts"](#) on page 302

## Alert 3103

**Cluster <cluster>: The server certificate will expire within <count> days. All system access may be lost.**

The specified cluster's server certificate will soon expire. 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're logged into that cluster, click the link to go to the **Certificates** page. If not, log into that cluster and go to **Admin > Local Cluster > Certificates**.

See also:

["Alerts"](#) on page 302

## Alert 3104

**Cluster <cluster>: One or more CA certificates have expired.**

The specified cluster has an expired CA certificate or certificates. 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're logged into that cluster, click the link to go to the **Certificates** page. If not, log into that cluster and go to **Admin > Local Cluster > Certificates**.

If that cluster has **Skip certificate validation for user login sessions** turned off, you won't be able to log into it. Contact Polycom Global Services.

See also:

[“Alerts”](#) on page 302

## Alert 3105

### **Cluster <cluster>: One or more CA certificates will expire within 30 days.**

The specified cluster has a CA certificate or certificates that will expire soon. 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're logged into that cluster, click the link to go to the **Certificates** page. If not, log into that cluster and go to **Admin > Local Cluster > Certificates**.

See also:

[“Alerts”](#) on page 302

## Alert 3201

### **Cluster <cluster> requires license activation. Apply license key(s).**

You haven't entered the license key(s) for the specified cluster.

If you're logged into that cluster, click the link to go to the **Licenses** page. If not, log into that cluster and go to **Admin > Local Cluster > Licenses**.

Without a valid license, the cluster is limited to ten simultaneous calls.

See also:

[“Alerts”](#) on page 302

## Alert 3202

### **Invalid license keys applied to cluster <cluster>. System will allow 10 calls.**

The specified cluster has an invalid license key or keys.

If you're logged into that cluster, click the link to go to the **Licenses** page. If not, log into that cluster and go to **Admin > Local Cluster > Licenses**.

Without a valid license, the cluster is limited to ten simultaneous calls.

See also:

[“Alerts”](#) on page 302

## Alert 3301

**Cluster <cluster> is configured for 2 nodes, but only a single node is detected.**

One of the servers in the specified cluster is not responding to the other server over the private network that connects them.

This could be a hardware problem, or the server in question may just need to be rebooted. It's also possible that the private network connection between the two servers has failed. Check the ethernet cable connecting the GB2 ports and replace it if necessary.

See also:

[“Alerts”](#) on page 302

## Alert 3302

**Cluster <cluster> is configured for 1 node, but the private interface is enabled and active.**

Either the cluster contains two servers but was misconfigured as a single-node cluster, or there is only one server in the cluster but something is connected its GB2 port.

On a single-node cluster, don't use the server's GB2 port for anything.

See also:

[“Alerts”](#) on page 302

## Alert 3303

**Cluster <cluster>: A private network error exists on <server>.**

The specified server has detected a problem with the private network that connects the two servers in the cluster.

This could be a problem with the GB2 port (eth1 interface) or the ethernet cable connecting the GB2 ports. Or the server in question may just need to be rebooted.

See also:

[“Alerts”](#) on page 302

## Alert 3304

**Cluster <cluster>: A management network error exists on <server>.**

The specified server has detected a problem with the management (or combined management and signaling) network connection.

This could be a problem with the GB1 port (eth0 interface), 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.

See also:

[“Alerts”](#) on page 302

## Alert 3305

**Cluster <cluster>: A signaling network error exists on <server>.**

The specified server has detected a problem with the signaling network connection.

This could be a problem with the GB3 port (eth2 interface), 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.

See also:

[“Alerts”](#) on page 302

## Alert 3401

**Cluster <cluster>: Available disk space is less than 15% on server <server>.**

The specified cluster is running out of disk space.

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 isn't being repeatedly backed up.
- Roll logs more often (compressing the data) and make sure **Logging level** is set to **Production**.

See also:

[“Alerts”](#) on page 302

## Alert 3402

**Cluster <cluster>: Old log files on server <server> will be purged within <timeframe>.**

Log archives on the specified cluster are approaching the retention limit set on the **Logging Settings** page.

Click the link to go to the **System Log Files** page. We recommend routinely downloading archived logs and then deleting them from the system.

See also:

[“Alerts”](#) on page 302

## Alert 3403

**Cluster <cluster>: Log files on server <server> exceed the capacity limit and will be purged within 24 hours.**

Log archives on the specified cluster exceed the 1 GB capacity limit for logs. After midnight, the system will delete sufficient log archives to get below the 1 GB 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.

See also:

[“Alerts”](#) on page 302

## Alert 3404

**Cluster <cluster>: Log files on server <server> are close to capacity limit and may be purged within 24 hours.**

Log archives on the specified cluster have reached the percentage of capacity that triggers an alert, set on the **Logging Settings** page.

Click the link to go to the **System Log Files** page. We recommend routinely downloading archived logs and then deleting them from the system.

See also:

[“Alerts”](#) on page 302

## Alert 3405

**Server <server> CPU utilization >50% and <75%.**

The specified server’s CPU and/or I/O bandwidth usage is unusually high.

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 **Maintenance > 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.

See also:

[“Alerts”](#) on page 302

## Alert 3406

### **Server <server> CPU utilization > 75%.**

The specified server’s CPU and/or I/O bandwidth usage is exceptionally high.

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 **Maintenance > 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.

See also:

[“Alerts”](#) on page 302

## Alert 3601

### **Cluster <cluster>: System version differs between servers.**

The specified cluster is supposed to have two nodes, but a software version mismatch makes it impossible for them to form a redundant two-server cluster.

Possible explanations:

- Someone upgraded one node of the cluster while the other was turned off or otherwise unavailable.
- An expansion node was added to a single-node cluster, but the new server wasn’t patched to the same software level as the existing server.
- An RMA replacement server wasn’t patched to the same software level as the existing server.

If you’re logged into that cluster, click the link to go to the **Software Upgrade** page. If not, log into that cluster and go to **Maintenance > 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.

See also:

[“Alerts”](#) on page 302

## Alert 3602

**Cluster <cluster>: Local time differs by more than ten seconds between servers.**

The time on the two servers in the specified cluster has drifted apart by an unusually large amount. This may indicate a misconfiguration or a problem with one of the servers. Contact Polycom Global Services.

See also:

[“Alerts”](#) on page 302

## Alert 3603

**Cluster <cluster>: Enterprise directory integration is not consistent between servers.**

In the specified cluster, the Active Directory integration status information is different on the two servers, indicating that their internal databases aren't consistent.

Try to determine which server's data is incorrect and reboot it.

See also:

[“Alerts”](#) on page 302

## Alert 3604

**Cluster <cluster>: Enterprise conference rooms differ between servers.**

In the specified cluster, the enterprise conference room counts are different on the two servers, indicating that their internal databases aren't consistent.

Try to determine which server's data is incorrect and reboot it.

See also:

[“Alerts”](#) on page 302

## Alert 3605

**Cluster <cluster>: Custom conference rooms differ between servers.**

In the specified cluster, the custom conference room counts are different on the two servers, indicating that their internal databases aren't consistent.



Try to determine which server's data is incorrect and reboot it.

See also:

["Alerts"](#) on page 302

## Alert 3606

### **Cluster <cluster>: Local users differ between servers.**

In the specified cluster, the local users are different on the two servers, indicating that their internal databases aren't consistent.

Try to determine which server's data is incorrect and reboot it.

See also:

["Alerts"](#) on page 302

## Alert 4001

### **MCU "<MCUname>" is currently busied out.**

Someone busied out the specified MCU.

Click the link to go to the **MCUs** page.

See also:

["Alerts"](#) on page 302

## Alert 4002

### **MCU "<MCUname>" is currently out of service.**

Someone took the specified MCU out of service.

Click the link to go to the **MCUs** page.

See also:

["Alerts"](#) on page 302

## Alert 4003

### **MCU "<MCUname>" has <count> warning(s).**

The **MCUs** page is displaying warnings related to the specified MCU.

Click the link to go to the **MCUs** page for more information.

See also:

[“Alerts”](#) on page 302

## Alert 5001

**<Model> ITP system attempting to register with ID <H.323 ID> is improperly configured.**

A device that identifies itself as an ITP (Immersive Telepresence) system has registered with the Call Server, but the H.323 ID of the device doesn't specify its endpoint number or the number of endpoints in the ITP system, as it should.

The H.323 ID must be updated on the endpoints of the ITP system.

See also:

[“Alerts”](#) on page 302

## Alert 6001

**No territories configured to host conference rooms.**

You must enable a territory to host conference rooms in order to use the cluster responsible for the territory as a Conference Manager. You can enable up to three territories to host conference rooms.

Click the link to go to the **Territories** page.

See also:

[“Alerts”](#) on page 302

## Alert 7001

**Failed registration data incomplete: <cluster> history limited to <n.n> hours.**

Registration data retention settings are too low for the system to determine the number of failed registrations in the past 24 hours.

Click the link to go to the **History Retention Settings** page and increase the number of registration records to retain on each cluster.

See also:

[“Alerts”](#) on page 302

## System Log Files

The **System Log Files** page lists the available system log file archives and lets you run the following **Action** list commands:

- **Roll 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 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, in the **File Download** dialog box you can select which node's logs to download.
- **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 have been downloaded can be deleted.
- **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 at **Admin > Local Cluster > Logging Settings**. See "[Logging Settings](#)" on page 63.

The archives are Gzip-compressed tar files. Each archive contains a number of individual log files.

The detailed technical data in the log files is not useful to you, but can help Polycom Global Services resolve problems and provide technical support for your system.

In such a situation, 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 in order to begin gathering data anew. After a certain amount of the activity of interest, you may be asked to download the active logs and send them to Polycom Global Services.

The following table describes the fields in the **System Log Files** list.

**Table 13-1** Information in the System Log Files list

Column	Description
Time	Date and time that the log file archive was created.
Host	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 node.

**Table 13-1** Information in the System Log Files list

Column	Description
Filename	Name of the log file archive.
Size	Size of the file in megabytes.
Type	Indicates whether this is an automatic archive, manual archive, or system snapshot archive (created when you download the active logs).

The following table describes the fields in the **Download History** list.

**Table 13-2** Information in the Download History list

Column	Description
User	The user ID of the person who downloaded the archive.
Time	Date and time that the archive was downloaded.

## System Logs Procedures

### To download a log archive to your PC or workstation

- 1** Go to **Maintenance > System Log Files**.  
The **System Log Files** page appears.
- 2** To download a listed log archive:
  - a** Select the file you want.
  - b** In the **Actions** list, click **Download Archived Logs**.
  - c** In the dialog box, select a location and click **Save**.
- 3** To download an archive of the currently open log files (but not close them):
  - a** In the **Actions** list, click **Download Active Logs**.
  - b** In the dialog box, specify a location and file name, and click **Save**.

### To manually roll the system logs

- 1** Go to **Maintenance > System Log Files**.  
The **System Log Files** page appears.
- 2** In the **Actions** list, click **Roll Logs**.  
If you have a supercluster, you're prompted to choose the cluster whose 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 box informs you that logs have been rolled, and the new log archive appears in the **System Log Files** list. For a two-node cluster, an archive is created for each node.

- 4 Click **OK**.

### To delete a system log archive

#### Note

Only users with the Auditor role can delete archives, and only archives that have been downloaded can be deleted.

- 1 Go to **Maintenance > System Log Files**.

The **System Log Files** page appears.

- 2 Select the log archive and verify that the **Show Download History** command appears, indicating that it has been downloaded at least once and can be deleted. Click the command to see the **Download History** list.

- 3 In the **Actions** list, click **Delete Archived Logs**.

A confirmation dialog box appears.

- 4 Click **Yes**.

See also:

["Management and Maintenance Overview"](#) on page 291

["Recommended Regular Maintenance"](#) on page 293

["Alerts"](#) on page 302

["Call Detail Records \(CDRs\)"](#) on page 344

## Troubleshooting Utilities

The Polycom DMA system's **Troubleshooting Utilities** submenu includes several useful network and system status commands, which you can run and view the output of in the system's familiar graphical interface. Each command is run on each server in the cluster, and the results are displayed in a separate panel for each server.

### Ping

Use **Ping** to verify that the Polycom DMA system's servers can communicate with another node in the network.

#### To run ping on each server

- 1 Go to **Maintenance > Troubleshooting Utilities > Ping**.
- 2 Enter an IP address or host name and click **Ping**.

The system displays results of the command for each server.

### Traceroute

Use **Traceroute** to see the route that the servers use to reach the address you specify and the latency (round trip) for each hop.

#### To run traceroute on each server

- 1 Go to **Maintenance > Troubleshooting Utilities > Traceroute**.
- 2 Enter an IP address or host name and click **Trace**.

The system displays results of the command for each server.

### Top

Use **Top** to see an overview of each server's current status, including CPU and memory usage, number of tasks, and list of running processes. The displays update every few seconds.

#### To run top on each server

- >> Go to **Maintenance > Troubleshooting Utilities > Top**.

The system displays results of the command for each server.

## I/O Stats

Use **I/O Stats** to see CPU resource allocation and read/write statistics for each server.

### To run iostat on each server

>> Go to **Maintenance > Troubleshooting Utilities > I/O Stats**.

The system displays results of the command for each server.

## SAR

Use SAR to see a system activity report for each server.

### To run sar on each server

>> Go to **Maintenance > Troubleshooting Utilities > SAR**.

The system displays results of the command for each server.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Recommended Regular Maintenance”](#) on page 293

# Backing Up and Restoring

Every night, the Polycom DMA system determines whether its configuration or local user data have changed. If so, it creates a backup of that data, plus the audit records as of the time of the backup, on each server. It keeps the most recent ten backups on each server (deleting the oldest backup file when a new one is created).

The Polycom DMA system’s **Backup and Restore** page lets you:

- Manually create a backup at any time.
- Download backup files from the server for safekeeping.
- Upload backup files to the server.
- Restore the system configuration and local user data from a specific backup file.

In addition, the Polycom DMA USB Configuration Utility (on the USB stick used to initially configure the network and system parameters) can restore the Polycom DMA system from a backup file that you load onto the USB stick.

**Note**

We strongly suggest that you:

- Download backup files regularly for safekeeping.
- Restore from a backup only when there is no activity on the system. Restoring terminates all conferences and reboots the system.
- For a two-server cluster, make system configuration changes, including restores, only when both servers are running and clustered.
- If the system is shut down or in a bad state, use the USB stick to restore.

The following table describes the fields in the **Backup and Restore** list.

**Table 13-3** *Information in the Backup and Restore list*

Column	Description
Creation Date	Timestamp of the backup file.
Name	Name of the backup file.
Size	Size of the backup file.
System Version	Version number of the application that created the backup file.
SHA1	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.

## Backup and Restore Procedures

**Caution**

Restoring from a backup requires a system restart and terminates all active conferences.

**Note**

You can restore the system while it's integrated with a Polycom CMA system, but the result depends on the state when the backup you're restoring from was made.

If the system was integrated with a Polycom CMA system when the backup you're restoring was made, that integration is restored. If the system wasn't integrated when the backup was made, it will no longer be integrated after restoring.

You can't restore a cluster while it's part of a supercluster. You must manually leave the supercluster first. If the cluster is responsible for any territories (as primary or backup), go to **Network > Site Topology > Territories** and reassign those territories.



**To download a backup file**

- 1 Go to **Maintenance > Backup and Restore**.  
The list contains the last ten backup files.
- 2 Select the backup file you want to download.
- 3 In the **Actions** list, click **Download Selected**.
- 4 Choose a path and filename for the backup file and click **Save**.  
The **File Download** dialog box indicates when the download is complete.
- 5 Click **Close**.

**To create a new backup file**

- 1 Go to **Maintenance > Backup and Restore**.
- 2 Verify that the oldest backup file listed is one you don't want to keep or have already downloaded.  
Only ten files are saved. Creating a new backup will delete the oldest file (unless there are fewer than ten).
- 3 In the **Actions** list, click **Create New**.  
A confirmation dialog tells you the backup archive was created.
- 4 Click **OK**.

**To upload a backup file**

- 1 Go to **Maintenance > Backup and Restore**.
- 2 Verify that the oldest backup file listed is one you don't want to keep or have already downloaded.  
Only ten files are saved. Uploading a backup will delete the oldest file (unless there are fewer than ten).
- 3 In the **Actions** list, click **Upload**.
- 4 Choose a backup file to upload and click **Open**.  
The **File Upload** dialog box 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 don't want to restore (and restart the system) now, click **Manually Later**. When you're ready to restore, use the procedure that follows this one.

- 7 To restore now, make sure you meet the criteria in the first step of the following procedure, and click **Now**. When asked to confirm, click **Yes**.

A dialog box informs you when all files have been restored.

- 8 Click **OK**.

The system logs you out and the server reboots (typically, this takes about five minutes). After it comes back up, in a two-server cluster, the second node syncs to it, thus being restored to the same state.

### To restore from a backup file on the server

- 1 If this is a two-server cluster, make sure that both nodes are running and clustered. Make sure that there are no calls on the system, and that all MCUs are out of service. See “[MCU Procedures](#)” on page 124.

- 2 Go to **Maintenance > Backup and Restore**.

- 3 Select the backup file from which you want to restore.

- 4 In the **Actions** list, click **Restore Selected**.

- 5 When asked to confirm that you want to restore, click **Yes**.

A dialog box informs you when all files have been restored.

- 6 Click **OK**.

The system logs you out and the server reboots (typically, this takes about five minutes). After it comes back up, in a two-server cluster, the second node syncs to it, thus being restored to the same state.

### To restore from a backup file on the Polycom DMA system’s USB stick

- 1 If the system is running and accessible, log in as an Administrator, make sure that there are no calls on the system and that all MCUs are out of service. See “[MCU Procedures](#)” on page 124.

- 2 Shut down the system. See “[Shutting Down and Restarting](#)” on page 337.

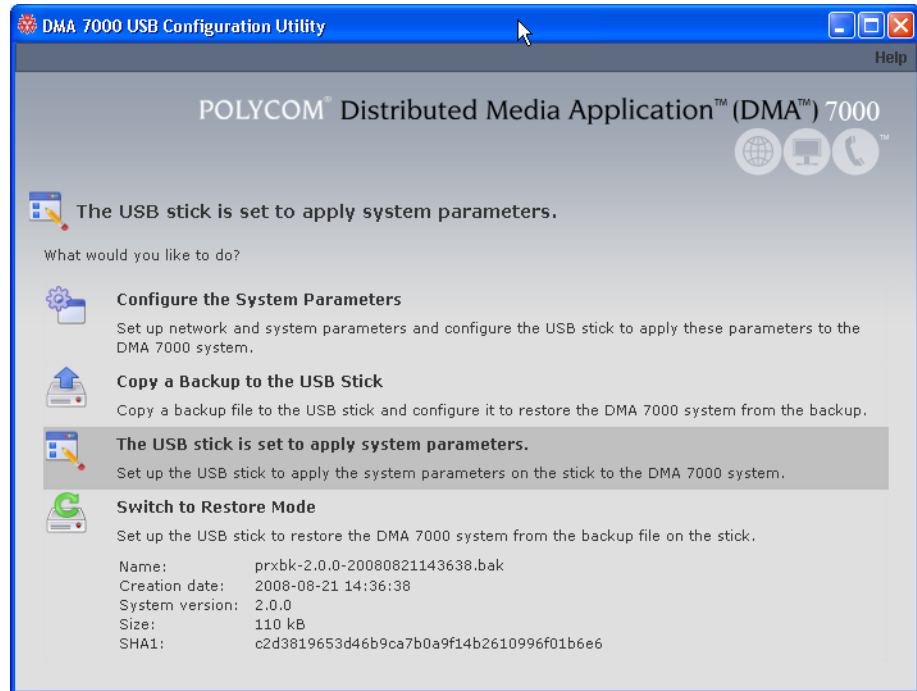
- 3 Connect the USB memory stick containing the DMA USB Configuration Utility (included with your Polycom DMA system) to a Windows PC.

- 4 When prompted, elect to run the DMA USB Configuration Utility.

#### Note

If autorun doesn’t work or is turned off, navigate to the USB memory stick using My Computer, Windows Explorer, or another file manager. Then start the Configuration Utility by double-clicking `dma7000-usb-config.exe`.

- 5 In the **DMA USB Configuration Utility** window, click **Copy a Backup to the USB Stick**.



- 6 Select the backup file from which you want to restore the system and click **Open**.

The utility displays an error message if the file isn't a valid Polycom DMA system backup. Otherwise, it confirms that the backup file is in place.

The utility's main window states that **The USB stick is ready to restore the system from a backup file**. At the bottom of the window, it displays information about the selected backup file.

- 7 Close the utility.
- 8 In your system tray, click **Safely Remove Hardware** and select **Safely Remove USB Mass Storage Device**. When a message tells you it's safe to do so, disconnect the USB memory stick from the PC and take it to the data center housing the Polycom DMA system server(s).
- 9 Make sure that the server or servers are turned off. Then insert the USB stick into a USB port on one of the servers and turn that node (but not the other, if there are two) on.

The server boots and the data in the backup file is applied. Typically, this takes about five minutes. Depending on the configuration changes being applied, the server may reboot so the changes can take effect.

- 10** If this is a two-server cluster, after the first node has rebooted (if necessary) and its front-panel LCD displays **DMA Ready**, turn on the second node.

The second node boots, finds the first node, and syncs to it, thus being restored to the same state. Depending on the configuration changes being applied, it may reboot so the changes can take effect.

When done, both servers' LCDs display **DMA Clustered**.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Recommended Regular Maintenance”](#) on page 293

## Upgrading the Software

The Polycom DMA system's **Software Upgrade** page lets you upload a software upgrade package and install the upgrade on your system (both servers, if present). It also lets you roll back to the previous version, if necessary.

This process can be used for patches, minor upgrades, and major upgrades. In all three cases, the current system configuration (including users, MCUs, Conference Manager settings, Call Server settings, and local cluster settings) is preserved.

Patches don't require new license keys, but major and minor version upgrades do. Any of the three may require a system restart. If so, that information is displayed on the page after you upload the upgrade package.

The following table describes the parts of the **Software Upgrade** page.

**Table 13-4** *Parts of the Software Upgrade page*

Field	Description
Version Information	Shows the current system version and the rollback version (if any), which is the previous system version.
Upgrade Package Details	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.
Operation History	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.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Recommended Regular Maintenance”](#) on page 293

[“Planning a Supercluster Upgrade”](#) on page 329

[“Upgrade Procedures”](#) on page 330

## Planning a Supercluster Upgrade

All the clusters in a supercluster must be running compatible software versions. Patch releases will generally be compatible, but major and minor version upgrades will not be compatible. An incompatible version software upgrade on all clusters in a supercluster requires a bit of planning, because it's not possible to upgrade a cluster to an incompatible software version while it's a member of the supercluster. Each cluster must be upgraded individually.

During the course of the upgrade, some clusters will be on the new software version while others are still on the older version, effectively creating two separate superclusters until all the clusters are upgraded.

### Caution

We strongly recommend upgrading a supercluster only during a maintenance window when there are no calls or conferences on the system.

At a minimum, ensure that there is no conferencing activity in any given territory until after both the primary and backup cluster for the territory have been upgraded, joined to the new supercluster, and reassigned their territory responsibilities.

To save time, upload the upgrade package to all clusters in the supercluster before beginning.

If you're planning to form a supercluster, we encourage you to upgrade to the latest version before doing so.

Before you start, determine the order in which the clusters will be upgraded. Then, proceed as follows (assuming five clusters, A-E):

- 1 Assuming cluster A is the one you've chosen to upgrade first, remove it from the supercluster. Then upgrade it as described in [“Upgrade Procedures”](#) on page 330.
- 2 Once cluster A is upgraded, remove cluster B (the next one in your plan) from the supercluster and upgrade it in the same way.
- 3 Once cluster B is upgraded, log into it, go to **Network > DMAs**, and create a new supercluster by joining cluster B to cluster A (if you encounter an error, reboot cluster B and try again).

You now have two superclusters, (A, B) and (C, D, E). Verify that the shared data (users, groups, MCUs, site topology, etc.) from the original supercluster is still preserved on supercluster (A, B).

- 4 If all is well, remove cluster C from supercluster (C, D, E), upgrade it, and join it to supercluster (A, B).
- 5 Do the same in turn for clusters D and E.

When finished, you should have a single upgraded supercluster.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Upgrading the Software”](#) on page 328

[“Upgrade Procedures”](#) on page 330

## Upgrade Procedures

### Note

The upgrade installation process automatically creates a backup, which enables you to roll back an upgrade (restore the previous version) if necessary. As a precaution, however, we recommend that you download a recent backup file before you begin to install an upgrade. See [“Backing Up and Restoring”](#) on page 323.

You can roll back only the last applied upgrade. Rolling back an upgrade restores the database to its state prior to the upgrade, so data may be lost.

To upgrade a superclustered system, first see [“Planning a Supercluster Upgrade”](#) on page 329.

Always check the upgrade version release notes before installing an upgrade.

### To install an upgrade

- 1 Put the upgrade package file somewhere on or accessible from your PC.
- 2 Go to **Maintenance > Software Upgrade**.
- 3 In the **Actions** list, click **Upload**.
- 4 Select the upgrade package file and click **Open**.

The **File Upload** dialog box indicates when the upload is complete.

- 5 Click **Close**.

The **Upgrade Package Details** section displays information about the file you uploaded. The description includes an estimated install time.

- 6 Verify that the upgrade package is correct. If a system restart is required, make sure that there are no calls on the system.

Most upgrades will require a restart.

- 7 If this cluster is part of a supercluster, do the following:
  - a Go to **Network > Site Topology > Territories** and reassign the cluster’s territory responsibilities.

- b** Go to **Network > DMAs** and take it out of service.
    - c** Return to **Maintenance > Software Upgrade**.
  - 8** In the **Actions** list, click **Upgrade**.  
A confirmation dialog box appears.
  - 9** Click **Yes**.  
If a restart is required, a dialog box informs you that the upgrade is starting. Shortly after that, the system logs you out and restarts.
  - 10** Click **OK** to log out immediately, or simply wait.  
When the upgrade process is finished, in a two-server cluster, both servers' LCDs display **DMA Clustered** (in a single-server system, the LCD displays **DMA Ready**), and you're able to log back in.
- Note**  
You may need to restart your browser or flush your browser cache in order to log back into the system.
- 11** Log back in 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 **Maintenance > Software Upgrade** and check the **Operation History** table.
  - 12** If this cluster is part of a supercluster, this is a compatible patch upgrade, and the upgrade failed, do the following:
    - a** Power off both servers of the cluster that failed to upgrade.
    - b** On another cluster in the supercluster, go to **Network > DMAs** and remove the failed cluster.
    - c** Re-install the failed cluster from media and upgrade its software to the same level as the rest of the supercluster.
    - d** Go to **Network > DMAs** and rejoin the failed cluster to the supercluster.
  - 13** If this cluster is part of a supercluster, this is a compatible patch upgrade, and the upgrade succeeded, do the following:
    - a** Go to **Network > DMAs** and put it back into service.
    - b** Go to **Network > Site Topology > Territories** and reassign territory responsibilities back to it.
  - 14** Call Polycom Global Services if:
    - After waiting significantly longer than the estimated install time, you're still unable to log back in.

- You can log in, but the **Dashboard** shows only one node for a two-server cluster.
- The package version numbers on the two nodes are not the same.

### To roll back an upgrade, restoring the previous version

- 1 Go to **Maintenance > Software Upgrade**.
- 2 Verify that you want to downgrade the system to the rollback version shown and that you're prepared for a system restart, if required.

Most rollbacks will require a restart.

- 3 In the **Actions** list, click **Roll Back**.

A confirmation dialog box appears.

- 4 Click **Yes**.

If a restart is required, a dialog box informs you that the downgrade is starting. Shortly after that, the system logs you out and restarts.

- 5 Click **OK** to log out immediately, or simply wait.

When the downgrade process is finished, in a two-server cluster, both servers' LCDs display **DMA Clustered** (in a single-server system, the LCD displays **DMA Ready**), and you're able to log back in.

#### Note

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

- 6 Log back in 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 **Maintenance > Software Upgrade** and check the **Operation History** table.
  - c Go to **Network > MCU > MCUs** and put the MCUs back into service. See "[MCU Procedures](#)" on page 124.
- 7 If this cluster is part of a supercluster, this is a compatible patch upgrade, and the upgrade failed, do the following:
  - a Power off both servers of the cluster that failed to upgrade.
  - b On another cluster in the supercluster, go to **Network > DMAs** and remove the failed cluster.
  - c Re-install the failed cluster from media and upgrade its software to the same level as the rest of the supercluster.
  - d Go to **Network > DMAs** and rejoin the failed cluster to the supercluster.



- 8 If this cluster is part of a supercluster, this is a compatible patch upgrade, and the upgrade succeeded, do the following:
  - a Go to **Network > DMAs** and put it back into service.
  - b Go to **Network > Site Topology > Territories** and reassign territory responsibilities back to it.
- 9 Call Polycom Global Services if:
  - After waiting significantly longer than the estimated install time, you're still unable to log back in.
  - You can log in, but the **Dashboard** shows only one node for a two-server cluster.
  - The package version numbers on the two nodes are not the same.

See also:

["Management and Maintenance Overview"](#) on page 291

["Upgrading the Software"](#) on page 328

["Planning a Supercluster Upgrade"](#) on page 329

## Adding a Second Server

A single-server Polycom DMA system can be upgraded to a fault-tolerant two-server cluster at any time. For an overview of how a two-server cluster works and its advantages, see ["Two-server Cluster Configuration"](#) on page 2.

To form a two-server cluster, both servers must be running the same version of the Polycom DMA system software. Depending on the software level of your existing server, you can accomplish this in one of two ways:

- If your existing server is running an unpatched release version of the system software for which you have the installation DVD, follow the procedure in ["Expanding an Unpatched System"](#) on page 334.
- If your existing server is running a patched version of the system software different from that on the installation DVD, follow the procedure in ["Expanding a Patched System"](#) on page 335.

Both procedures assume that you've ordered and received the server expansion package, which includes the second server, its accessories, and a new License Certificate.

See also:

["Management and Maintenance Overview"](#) on page 291

["Recommended Regular Maintenance"](#) on page 293

["Expanding an Unpatched System"](#) on page 334

["Expanding a Patched System"](#) on page 335

## Expanding an Unpatched System

### To expand an unpatched single-server system into a two-server cluster

- 1 Unpack, inspect, and physically install the second server as described in its *Getting Started Guide*. Mount it in the rack adjacent to the first Polycom DMA system server (or close enough to connect them with one of the provided crossover Ethernet cables).
- 2 Log into your Polycom DMA system, go to **Admin >Local Cluster > Network Settings**, and add the Node 2 host name and IP address for the second server. See [“Network Settings”](#) on page 54.

The first server (Node 1) reboots.

- 3 Connect the second server to the network:
  - a Connect the GB 1 Ethernet port of the new server to the enterprise network.
  - b Use one of the provided crossover cables to connect the GB 2 ports of the two servers.

#### Caution

The first server must be running properly before you turn on the second server.

- 4 Confirm that the first server is running and displays **DMA Ready**. Then turn on the second server, insert the installation DVD, and reboot it.  
  
The server boots from the DVD, and the installation commences. About 15-20 minutes later, the DVD ejects and the server reboots. It detects the presence of Node 1, gets its configuration settings from it, and joins the cluster. When done, both servers' LCDs display **DMA Clustered**.
- 5 Log into the system, go to **Admin >Local Cluster > Licenses**, and follow the procedure for obtaining and entering a license activation key. See [“Add Licenses”](#) on page 64.
- 6 On the **Dashboard**, check the **License Status**, **Supercluster Status**, and **Cluster Info** panes to verify that you now have a properly configured two-server cluster.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Adding a Second Server”](#) on page 333

[“Expanding a Patched System”](#) on page 335

## Expanding a Patched System

### To expand a patched single-server system into a two-server cluster

- 1 Unpack, inspect, and physically install the second server as described in its *Getting Started Guide*. Mount it in the rack adjacent to the first Polycom DMA system server (or close enough to connect them with one of the provided crossover Ethernet cables).
- 2 Connect the GB 1 Ethernet port of the new server to the enterprise network. Don't connect the crossover cable between the two servers at this time.
- 3 Log into your existing Polycom DMA system and determine the software version (including patch level) installed on the first (existing) server. Write it down for later reference.
- 4 Go to **Admin >Local Cluster > Network Settings**, and add the Node 2 host name and IP address for the second server. See ["Network Settings"](#) on page 54.

The first server (Node 1) reboots.

- 5 Shut down the first server (Node 1).
- 6 Using the USB Configuration Utility and the procedure in the *Getting Started Guide*, complete the installation and initial configuration of the new server as a stand-alone single-server system. If necessary, use your installation DVD to install the same release version of the software that's on your first server.

#### Caution

Assign the new server its own real and virtual IP addresses. Don't assign it the virtual IP address of the existing system.

- 7 Log into the new server, go to **Maintenance > Software Upgrade**, and install the patch(es) needed to make it match the software version on the first server. See ["Upgrading the Software"](#) on page 328.
- 8 Shut down the new server. See ["Shutting Down and Restarting"](#) on page 337.
- 9 Use one of the provided crossover cables to connect the GB 2 ports of the two servers.
- 10 Turn on the first server (Node 1).

#### Caution

The first server must be running properly before you turn on the second server.

- 11** When the first server displays **DMA Ready**, turn on the second server.  
The second server boots, detects the presence of Node 1, gets its configuration settings from it, and joins the cluster. When done, both servers' LCDs display **DMA Clustered**.
- 12** Log into the system, go to **Admin >Local Cluster > Licenses**, and follow the procedure for obtaining and entering a license activation key. See ["Add Licenses"](#) on page 64.
- 13** On the **Dashboard**, check the **License Status**, **Supercluster Status**, and **Cluster Info** panes to verify that you now have a properly configured two-server cluster.

See also:

["Management and Maintenance Overview"](#) on page 291

["Adding a Second Server"](#) on page 333

["Expanding an Unpatched System"](#) on page 334

## Replacing a Failed Server

Replacing a server is essentially the same process as adding a second server to a single-server system. As in that situation, you must make sure that both servers are running the same version of the Polycom DMA system software.

The procedure assumes that you've gone through the RMA process and received the replacement server package, which includes the server, its accessories, and a new License Certificate.

### To replace a failed server in a two-server cluster

- 1** If you haven't already done so, power down, uncable, and remove the failed server.
- 2** Log into your Polycom DMA system and determine the software version (including patch level) installed on the remaining server. Write it down for later reference.
- 3** Do one of the following:
  - If your system is running an unpatched release version of the system software for which you have the installation DVD, follow the procedure in ["Expanding an Unpatched System"](#) on page 334, skipping step 2.
  - If your system is running a patched version of the system software different from that on the installation DVD, follow the procedure in ["Expanding a Patched System"](#) on page 335, skipping steps 3 and 4.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Recommended Regular Maintenance”](#) on page 293

## Shutting Down and Restarting

The Polycom DMA system’s **Shutdown and Restart** page lets you restart the system or turn it off completely. These commands affect both servers in a two-server cluster.

Both shutting down and restarting will terminate all existing calls and log out all current users.

### To restart or shut down both servers

- 1 Go to **Maintenance > Shutdown and Restart**.
- 2 Do one of the following:
  - To restart the system, click **Restart**.
  - To shut down the system (turn off both servers), click **Shut Down**.
- 3 When asked to confirm that you want to restart or shut down, click **Yes**.

The system logs you out and each server shuts down. If you chose **Restart**, the server(s) reboot, and conference service becomes available again when the restart is complete (typically, this takes about five minutes).

If you chose **Shut Down**, the server(s) remain powered off until you manually turn them back on.

See also:

[“Management and Maintenance Overview”](#) on page 291

[“Recommended Regular Maintenance”](#) on page 293



---

# System Reports

This chapter describes the following Polycom® Distributed Media Application™ (DMA™) 7000 system reports topics:

- [Alert History](#)
- [Call History](#)
- [Conference History](#)
- [Call Detail Records \(CDRs\)](#)
- [Registration History Report](#)
- [Active Directory Integration Report](#)
- [Orphaned Groups and Users Report](#)
- [Conference Room Errors Report](#)
- [Enterprise Passcode Errors Report](#)
- [Network Usage Report](#)

## Alert History

The **Alert History** page lets you view all the system alerts for the time period you select.

The search pane above the list lets you find alerts matching the criteria you specify. Click the down arrow to expand the search pane. You can search by description, alert code, or time period. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

The **Alert History** page lists the alerts matching the specified search criteria (up to 500). For each alert, it shows the start and end time, alert code, and description.

See also:

[“System Reports”](#) on page 339

## Call History

The **Call History** page lets you view detailed records of calls and download CDRs (call detail records). The list includes point-to-point calls through Call Server and VMR calls through Conference Manager.

The search pane above the list lets you find calls matching the criteria you specify. Click the down arrow to expand the search pane. You can search for an originator or destination device by its name, alias, or IP address.

The **Start After** and **Start Before** settings are always active and define the time range during which the calls to find begin. Optionally, use **End Before** to find only calls that ended by the specified time. Use **End After** to find calls that extended beyond the specified time; this is useful for finding very long calls. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

### Note

You can also access the call history of a specific device by selecting it on the **Endpoints** page and clicking **View Call History**.

After you search for calls, the **Call History** page lists the calls 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 **Show Call Details** command (in the **Actions** list) opens the **Call Details** dialog box, which provides detailed information about the selected call. See [“Call Details Dialog Box”](#) on page 71

When you select a call associated with a conference, the **Display Conference** command lets you switch from the **Call History** page to the **Conference History** page, displaying the associated conference.

The following table describes the fields in the list.

**Table 14-1** Information in the Call History list

Column	Description
From	Source of the call.
To	Destination of the call.
Call ID	Unique identifier for the call.
Start Time	Time the call began (first signaling event).
End Time	Time the call ended (session closed).
Host	Host name of the server that handled the call.



## Export History

The **Export History** list provides a record of the CDR exports (call and conference data downloads) from the system. It appears when you click the **Show Export History** command (in the **Actions** list). The following table describes the fields in the list.

**Table 14-2** Information in the Export History list

Column	Description
User	User ID of the person who performed the CDR export.
Date of Export	Date and time of the export.
Export Time Frame Start Date	Identify the time period for which CDRs were included in the export.
Export Time Frame End Date	

See also:

[“System Reports”](#) on page 339

[“Conference History”](#) on page 341

## Conference History

The **Conference History** page lets you view detailed records of conferences and download CDRs (call detail records).

The fields at the top of the page let you specify the starting and ending date and time or the conference room number (VMR number) 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 14-3** Information in the Conferences list

Column	Description
Conference ID	The conference room ID.
Start Time	Time the conference began (first conference event).
End Time	Time the conference ended (last conference event).
Host	Host name of server that handled the conference.

## Export History

The **Export History** list provides a record of the CDR exports (call and conference data downloads) from the system. It appears when you click the **Show Export History** command (in the **Actions** list). The following table describes the fields in the list.

**Table 14-4** Information in the Export History list

Column	Description
User	User ID of the person who performed the CDR export.
Date of Export	Date and time of the export.
Export Time Frame Start Date	Identify the time period for which CDRs were included in the export.
Export Time Frame End Date	

## Associated Calls

The **Associated Calls** list shows all the calls associated with the selected conference. The list displays the same data as described in [“Call History”](#) on page 340.

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 14-5** Information in the Conference Events list

Column	Description
Name	Name of the event.
Attributes	Information about the event (varies with the event type).
Call UUID	Call identifier (if call event).
Time	Date and time of the event.
Sequence	Identifies when in the order of changes to this conference this event occurred.

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 course of the conference. The following table describes the fields in the list.

**Table 14-6** Information in the Property Changes list

Column	Description
Name	Name of the call property.
Value	Value assigned to the property.
Time	Date and time of the property change.
Sequence	Identifies when in the order of changes to this call this property change occurred.

See also:

[“System Reports”](#) on page 339

[“Call History”](#) on page 340

[“Call Detail Records \(CDRs\)”](#) on page 344

## Call Detail Records (CDRs)

In addition to the online call and conference history reports, the Polycom DMA system generates call detail records (CDRs) for all calls and conferences, which you can download.

The procedure for exporting CDRs and the record layouts are described in the sections that follow.

### Exporting CDR Data

From the **Call History** or **Conference History** page, you can use the **Export CDR Data** command to download call detail records (CDRs) for the time period you specify.

#### To download CDRs

- 1 Go to **Reports > Call History** (or **Conference History**).
- 2 In the **Actions** list, click **Export CDR Data**.
- 3 In the **Export Time Frame** dialog box, set the **Start Date** and time and the **End Date** and time you want to include.

The defaults provide all CDR data for the current day.

- 4 Click **OK**.

A **Save** dialog box prompts you to select a location for the downloaded file. The default filename is `cdrExport.zip`, but you can change that.

- 5 Choose a path and filename for the CDR file and click **Save**.

The **File Download** dialog shows the progress.

- 6 When the download is complete, click **Close**.

After you unzip the download file, you can open the two CSV files it contains (one for calls and one for conferences) with Microsoft Excel or another spreadsheet application. The CSV files contain a line for each call or conference during the selected time frame. The Zip file also includes a text file that contains record counts and specifies the cluster(s) included.

### Call Record Layouts

The following table describes the fields in the call records.

Field values are enclosed in double quotes if:

- 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 14-7** Call CDR

Field	Description
version	Changes each time the format of CDRs changes (initially "1").
type	CALL
callType	One of the following: <ul style="list-style-type: none"> <li>• PT-PT</li> <li>• VMR</li> <li>• VEQ</li> <li>• VSC-hunt group</li> <li>• VSC-[uncond fwd   fwd busy   fwd no answer]</li> </ul>
callUuid	Call UUID MSB and call UUID LSB.
startTime	YYYY-MM-DD HH:MM:SS GMT+/-H[:MM] If multiple call records, the start of this segment of the call.
endTime	YYYY-MM-DD HH:MM:SS GMT+/-H[:MM] If multiple call records, the end of this segment of the call.
origEndpoint	The originating endpoint's name, display name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling.
dialString	Initial dial string as supplied by the originator. If multiple call records, this value is the same across all segments of the call.
destEndpoint	The destination endpoint's name, display name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling. If the destination is a VMR or VEQ, the VMR or VEQ number; if a VSC, the VSC value (not including the VSC).
origSignalType	One of the following: <ul style="list-style-type: none"> <li>• h323</li> <li>• sip</li> </ul>
destSignalType	One of the following: <ul style="list-style-type: none"> <li>• h323</li> <li>• sip</li> </ul>
refConfUUID	If VMR, conf uuid appearing in Conference CDR.
lastForwardEndpoint	If call forwarding, endpoint that forwarded call to the final destination endpoint.

**Table 14-7** Call CDR (continued)

Field	Description
cause	Cause value for call termination or termination of this CDR. This may not be the end of the call.
causeSource	Source of the termination of the call record: <ul style="list-style-type: none"> <li>• originator</li> <li>• destination</li> <li>• callserver</li> </ul>
bitRate	Bit rate for call, in kbps.
classOfService	Class of service for the call: <ul style="list-style-type: none"> <li>• Gold</li> <li>• Silver</li> <li>• Bronze</li> </ul>
ingressCluster	Virtual cluster ID; the cluster of the originating endpoint or entry point from a neighbor or SBC.
egressCluster	Virtual cluster ID; the cluster of the destination endpoint or exit point to a neighbor or SBC.
VMRCluster	Virtual cluster ID; the cluster handling the VMR, or blank if no VMR.
VEQCluster	Virtual cluster ID; the cluster handling the VEQ, or blank if no VEQ.
userDataA	User or provisioned data. Not currently used.
userDataB	User or provisioned data. Not currently used.
userDataC	User or provisioned data. Not currently used.

## Conference Record Layouts

The following table describes the fields in the conference records.

Values are enclosed in double quotes when necessary, using the same rules as for conference records.

**Table 14-8** Conference CDR

Field	Description
version	Changes each time the format of CDRs changes (initially "1").
type	CONF
confType	One of the following: <ul style="list-style-type: none"> <li>AD-HOC</li> <li>PCO (for calendared)</li> </ul>
cluster	Virtual cluster ID; the cluster serving the VMR.
confUUID	Unique identifier for the conference.
startTime	YYYY-MM-DD HH:MM:SS GMT+/-H[:MM]
endTime	YYYY-MM-DD HH:MM:SS GMT+/-H[:MM]
userID	User ID of the conference room (VMR) owner.
roomID	Conference room (VMR) number.
partCount	Maximum number of calls in the conference (high water mark).
classOfService	Class of service for the call: <ul style="list-style-type: none"> <li>Gold</li> <li>Silver</li> <li>Bronze</li> </ul>
userDataA	User or provisioned data. Not currently used.
userDataB	User or provisioned data. Not currently used.
userDataC	User or provisioned data. Not currently used.

See also:

["System Reports"](#) on page 339

["Call History"](#) on page 340

["Conference History"](#) on page 341

## Registration History Report

If the Polycom DMA system Call Server is providing H.323 gatekeeper or SIP registrar services, the **Registration History** page provides access to information about registered devices. It also provides information about external SIP peers with which the system is registered, if any.

The search pane above the list lets you find registrations matching the criteria you specify. Click the down arrow to expand the search pane.

The start and end time options provide complete flexibility in defining the time range in which you're interested, letting you specify registration start time criteria, registration end time criteria, or both. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

### Note

You can also access the registration history of a specific device by selecting it on the **Endpoints** page and clicking **View Registration History**.

The registrations that match your search criteria are listed below the search fields. In the **Actions** list, the **Show Details** command displays 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, and a history of the registration signaling and processing, including the results of applying the registration policy script, if any (see "[Registration Policy](#)" on page 227).

The following table describes the fields in the list.

**Table 14-9** Information in the Registration History list

Column	Description
Name	The name of the registered device.
Alias	The device's alias.
Start Time	The time and date that the device registered.
End Time	The time and date that the device's registration ended (blank if the device is still registered).
Registration Status	The registration status: <ul style="list-style-type: none"> <li>• Active</li> <li>• Rejected</li> <li>• Terminated by call server</li> <li>• Terminated by endpoint</li> <li>• Timed out</li> </ul>



## Registration History Procedures

### To find a device or devices

- 1 Go to **Reports > Registration History**.

The **Registration History** page appears.

- 2 For a simple search of the current day's registration history, enter a search string in the **Alias**, **Owner**, or **IP address** field. Select **Status**, **Protocol Type**, or **Device Type** values to apply those filters. Then 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. Leave a field empty to match all values. To search for a string not at the beginning of the field, you can use an asterisk (\*) as a wildcard.

- 3 To search by site or territory and specify a date range, click the down arrow to the right. Enter a search string in the **Site** or **Territory** field, set the date range you want, and click **Search**.

The system displays the devices matching your search criteria.

See also:

["System Reports"](#) on page 339

["Call History"](#) on page 340

["Conference History"](#) on page 341

## Active Directory Integration Report

If the Polycom DMA system is integrated with your Active Directory, it reads the Active Directory daily to refresh the information in its cache. It also rereads the directory whenever you update the directory integration settings (**Admin > Integrations > Microsoft Active Directory**).

For each cache update, the system generates an integration report.

The **Active Directory Integration** page reports the status for the last cache update, shows contact results for each domain in the forest, and lists any groups for which it was unable to retrieve membership information.

### Note

You must be an enterprise user (with the appropriate user role assignments) to see the Active Directory integration report. A local user can't access this page, regardless of user roles.

The following table describes the information displayed at the top of the page and the fields in the two lists.

**Table 14-10** *Fields on the Active Directory Integration page*

Field	Description
Status	<b>OK</b> indicates that the cluster successfully connected to the Active Directory during the last update. A padlock indicates that the connection was encrypted.
User and group cache	Shows the state of the cluster's cache of directory data and when it was last updated.
Server name	The Active Directory server from which the Polycom DMA system retrieved the directory data it needs.
Connected to global catalog	Indicates whether the cluster connected to a global catalog server. If it did, but some attributes were not in the global catalog, that's noted. Those attributes were retrieved from the domain controllers, and the results of that process are reported in the <b>All Domains</b> list below.
Forest root DN	Shows the distinguished name of the Active Directory forest root domain.
Site	<p>The Active Directory site name for the system. Available only if <b>Auto-discover from FQDN</b> (serverless bind) is selected on the <a href="#">Microsoft Active Directory Integration</a> page.</p> <p>If serverless bind is enabled, but no site is retrieved, the reason could be:</p> <ul style="list-style-type: none"> <li>• <b>Site could not be determined:</b> the system's subnet isn't mapped to a site (see <a href="http://support.microsoft.com//kb/889031">http://support.microsoft.com//kb/889031</a>).</li> <li>• <b>Auto-discover failed or is disabled:</b> could be problem with DNS domain name or missing SRV records on DNS server.</li> </ul>
<b>All Domains</b>	
Domain Name	Name of the domain. All domains in the forest are listed, whether or not they're used by the system.
Domain DN	Distinguished name of the domain.
Domain Server	Fully qualified domain name of the server.

**Table 14-10** Fields on the Active Directory Integration page (continued)

Field	Description
Status	<p>Indicates if the system contacted a domain controller in that domain (in order to retrieve attributes not in the global catalog or to get member information for its global groups) and the results:</p> <ul style="list-style-type: none"> <li>• <b>Not required:</b> no groups from that domain have been imported into the Polycom DMA system and all attributes needed were in the global catalog.</li> <li>• <b>Partially loaded</b> or <b>Unable to load:</b> see <b>Error Message</b> and the list of groups with incomplete information for more details.</li> </ul> <p>Displays an error message if the domain server couldn't be contacted. This can happen if the DNS server resolves the name to an IP address that isn't valid or is temporarily unavailable. Return to the <b>Active Directory Integration</b> page and try again.</p> <p>If the system repeatedly fails to contact a domain, troubleshoot your network.</p>
<b>Groups with Partially Loaded or No Membership Information</b>	
Group Name	<p>Name of a global group whose member information is incomplete. This includes groups that directly or indirectly contain groups whose member information is incomplete.</p> <p>Groups with members in multiple domains that couldn't be contacted are listed for each.</p>
Domain	Domain to which the group belongs.
Description	Description of the group.

See also:

["Microsoft Active Directory Integration"](#) on page 135

["Active Directory Integration Procedure"](#) on page 141

["Orphaned Groups and Users Report"](#) on page 352

["Conference Room Errors Report"](#) on page 353

["Enterprise Passcode Errors Report"](#) on page 355

## Orphaned Groups and Users Report

If the Polycom DMA system is integrated with your Active Directory, it generates an orphaned groups and users report whenever you manually update the directory connection (**Admin > Integrations > Microsoft Active Directory**) and when the system updates automatically to refresh its cache.

The **Orphaned Groups and Users** page reports information about enterprise users and groups that are no longer in the Active Directory or are no longer accessible to the Polycom DMA system, but for which the system has local data (typically, local conference rooms or customized enterprise conference rooms).

Orphaned data is no longer usable by the system, so you can generally delete it. But 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.

The following table describes the fields in the two lists.

**Table 14-11** Fields on the Orphaned Groups and Users page

Field	Description
<b>Orphaned Groups</b>	
Group ID	ID of the user group.
Domain	Domain to which the user group belonged.
<b>Orphaned Users</b>	
User ID	ID of the user.
First Name	The user's first name.
Last Name	The user's last name.
Domain	Domain to which the user belonged.
Roles	Polycom DMA system user roles assigned to the user.
Conference Rooms	Polycom DMA system custom conference rooms assigned to the user.

## Orphaned Groups and Users Procedures

### To remove orphaned group data from the system

- 1 Go to **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.

**To remove orphaned user data from the system**

- 1 Go to **Reports > Orphaned Groups and Users**.
- 2 In the **Actions** list, click **Clean Orphaned Users**.
- 3 When prompted to confirm, click **OK**.

The system removes the orphaned user data.

See also:

[“Microsoft Active Directory Integration”](#) on page 135

[“Active Directory Integration Report”](#) on page 349

[“Conference Room Errors Report”](#) on page 353

[“Enterprise Passcode Errors Report”](#) on page 355

## Conference Room Errors Report

If the Polycom DMA system is integrated with your Active Directory, it can create a conference room (virtual meeting room) for each enterprise user. See [“Microsoft Active Directory Integration”](#) on page 135.

The Polycom DMA system reads the Active Directory daily to refresh the information in its cache. It also rereads the directory whenever you update the directory integration settings (**Admin > Integrations > Microsoft Active Directory**).

If the directory integration settings are configured to generate conference room IDs for enterprise users, the Polycom DMA system retrieves the values from the designated directory attribute and removes the specified characters from them. If the resulting room ID is longer than the specified maximum, it strips the excess characters from the beginning of the string.

The **Conference Room Errors** page reports the conference room ID generation status and lists the problem IDs.

**Note**

You must be an enterprise user (with the appropriate user role assignments) to see the conference room errors report. A local user can't access this page, regardless of user roles.

The summary at the top of the report shows when it was generated (check this to verify that the report you're viewing reflects the most recent update of the cache) and the following information:

- Number of users in the directory
- Number of users with valid conference room IDs

If you don't specify a directory attribute from which to generate conference room IDs, this number is zero and the report contains nothing else of value.

- Number of users for whom the Active Directory field being used to generate conference room IDs is empty (these are counted, but not listed individually below; find them in the Active Directory)
- Number of blank conference room IDs (doesn't include those for whom the Active Directory field was empty, only those for whom its contents were filtered out)
- Number of invalid conference room IDs
- Number of duplicate conference room IDs

The blank, invalid, and duplicate conference room IDs are listed below.

#### Note

Duplicate conference room IDs are not disabled; they can be used for conferencing. But if both users associated with that conference room ID try to hold a conference at the same time, they end up in the same conference.

The following table describes the fields in the list.

**Table 14-12** Information in the Conference Room Errors list

Column	Description
Problem	Description of the issue with this room ID ( <i>Blank</i> , <i>Duplicate</i> , or <i>Invalid</i> ).
Conference Room ID	The conference room ID, typically generated from the enterprise user's phone number.
<directory attribute>	The attribute (field) from the Active Directory that's used to generate the room ID (see " <a href="#">Microsoft Active Directory Integration</a> " on page 135). The column heading is the name of the attribute, such as <b>telephoneNumber</b> .
User ID	The login name or ID of the enterprise user with this room ID.
Domain	The domain to which the enterprise user belongs.
Last Name	The enterprise user's last name.
First Name	The enterprise user's first name.
Notes	For duplicates, identifies the domain and user ID of the user with a duplicate conference room ID.

## Exporting Conference Room Errors Data

From the **Conference Room Errors** page, you can use the **Export Room Errors Report** command to download a CSV (comma-separated values) file containing all the data in the conference room errors report.

### To download conference room errors data

- 1 Go to **Reports > Conference Room Errors**.
- 2 In the **Actions** list, click **Export Room Errors Report**.
- 3 In the **Exporting Conference Room Errors Report** dialog box, click **Download**.
- 4 Choose a path and filename for the file and click **Save**.  
The **File Download** dialog shows the progress.
- 5 When the download is complete, click **Close**.

You can open the CSV file with Microsoft Excel or another spreadsheet application. The file contains the same data you see displayed on the **Conference Room Errors** page.

See also:

[“Microsoft Active Directory Integration”](#) on page 135

[“Active Directory Integration Report”](#) on page 349

[“Orphaned Groups and Users Report”](#) on page 352

[“Enterprise Passcode Errors Report”](#) on page 355

## Enterprise Passcode Errors Report

If the Polycom DMA system is integrated with your Active Directory, conference and chairperson passcodes for enterprise users can be maintained in the Active Directory. See [“Adding Passcodes for Enterprise Users”](#) on page 146.

The Polycom DMA system reads the Active Directory daily to refresh the information in its cache. It also rereads the directory whenever you update the directory integration settings (**Admin > Integrations > Microsoft Active Directory**).

If the directory integration settings are configured to generate passcodes for enterprise users, the Polycom DMA system retrieves the values from the designated directory attributes and removes any non-numeric characters from them. If the resulting numeric passcode is longer than the specified maximum for that passcode type, it strips the excess characters from the beginning of the string.

The **Enterprise Passcode Errors** page reports the passcode generation status and lists the users with passcode errors.

**Note**

You must be an enterprise user (with the appropriate user role assignments) to see the enterprise passcode errors report. A local user can't access this page, regardless of user roles.

The summary at the top of the report shows when it was generated (check this to verify that the report you're viewing reflects the most recent update of the cache), the directory server accessed, and the following information:

- Number of users in the directory
- Number of users with duplicate chairperson and conference passcodes

**Note**

For users with duplicate passcodes, the system ignores the conference passcode, but honors the chairperson passcode.

- Number of users with valid, invalid, and unassigned chairperson passcodes and the directory attribute on which they're based, along with the number of users with locally overridden chairperson passcodes
- Number of users with valid, invalid, and unassigned conference passcodes and the directory attribute on which they're based, along with the number of users with locally overridden conference passcodes

The users with invalid passcodes are listed below.

The following table describes the fields in the list.

**Table 14-13** Information in the Enterprise Passcode Errors list

Column	Description
Problem	Indicates what the problem is: Chairperson, Conference, or Duplicate.
User ID	The login name or ID of the enterprise user with this passcode error.
Domain	The domain to which the enterprise user belongs.



**Table 14-13** Information in the Enterprise Passcode Errors list (continued)

Column	Description
Last Name	The enterprise user's last name.
First Name	The enterprise user's first name.
Notes	For an invalid passcode, shows the generated value (after the system stripped non-numeric characters out of the attribute value and truncated it if necessary). For duplicate chairperson and conference passcodes, shows the raw attribute value of each and the duplicate value generated (after stripping non-numeric characters and truncating if necessary).

## Exporting Enterprise Passcode Errors Data

From the **Conference Room Errors** page, you can use the **Export Enterprise Passcode Errors Report** command to download a CSV (comma-separated values) file containing all the data in the enterprise passcode errors report.

### To download enterprise passcode errors data

- 1 Go to **Reports > Enterprise Passcode Errors**.
- 2 In the **Actions** list, click **Export Enterprise Passcode Errors Report**.
- 3 In the **Exporting Enterprise Passcode Errors Report** dialog box, click **Download**.
- 4 Choose a path and filename for the file and click **Save**.  
The **File Download** dialog shows the progress.
- 5 When the download is complete, click **Close**.

You can open the CSV file with Microsoft Excel or another spreadsheet application. The file contains the same data you see displayed on the **Enterprise Passcode Errors** page.

See also:

- ["Microsoft Active Directory Integration"](#) on page 135
- ["Adding Passcodes for Enterprise Users"](#) on page 146
- ["Active Directory Integration Report"](#) on page 349
- ["Orphaned Groups and Users Report"](#) on page 352
- ["Conference Room Errors Report"](#) on page 353

## Network Usage Report

The **Network Usage** page displays historical usage data about the video network and enables you to export that data.

The search criteria at the top of the page let you select:

- The start time and span/granularity you want included.
- The cluster, territory, or throttlepoint (site, site link, or subnet) whose data you want to see.
- The specific call, QoS, and bandwidth data you want to see.

The data matching the criteria you chose is graphed below.

## Exporting Network Usage Data

From the **Network Usage** page, you can use the **Export Network Usage Data** command to download a CSV (comma-separated values) file containing all the network usage data point records for the time period you specify.

The system retains the most recent 8 million data points.

The file includes a network usage data point record for each throttlepoint, territory, and cluster for each minute of the time period. 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 14-14** Network Usage record layout

Field	Description
Scope	The throttlepoint, territory, or cluster that is being measured.
Timestamp	Minutes since 1970 (Java time / 60,000).
Calls Started	Number of calls started in the scope during the time interval.
Calls Ended	Number of calls ended in the scope during the time interval.
Calls Dropped	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 bitrate limits at the throttlepoint.
Calls Downspeeded	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 bitrate limits at the throttlepoint.

**Table 14-14** Network Usage record layout (continued)

Field	Description
Bitrate Limit	The (maximum) configured bitrate limit for the scope during the time interval, or -1 if no limit was configured (kbps).
Bandwidth Limit	The (maximum) configured bandwidth limit for the scope during the time interval, or -1 if no limit was configured (kbps).
Bandwidth Usage	The (maximum) used bandwidth for the scope during the time interval (kbps).
Bandwidth Usage %	The (maximum) percentage of the bandwidth limit used for the scope during the time interval (kbps).
Packet Loss %	Mean packet loss percentage of all QoS reports in the scope during the time interval.
Avg Video Jitter	Mean jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Max Video Jitter	Maximum jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Avg Video Delay	Mean delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Max Video Delay	Maximum delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Avg Audio Jitter	Mean jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Max Audio Jitter	Maximum jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Avg Audio Delay	Mean delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Max Audio Delay	Maximum delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Gold Calls	Max concurrent Gold class calls in the scope during the time interval.
Silver Calls	Max concurrent Silver class calls in the scope during the time interval.
Bronze Calls	Max concurrent Bronze class calls in the scope during the time interval.
Audio Calls	Max concurrent audio calls in the scope during the time interval.
Calls 256kbps	Max concurrent video calls with a bitrate less than or equal to 320kbps in the scope during the time interval.
Calls 384kbps	Max concurrent video calls with a bit rate greater than 320kbps and less than or equal to 448kbps in the scope during the time interval.
Calls 512kbps	Max concurrent video calls with a bit rate greater than 448kbps and less than or equal to 640kbps in the scope during the time interval.

**Table 14-14** Network Usage record layout (continued)

Field	Description
Bitrate Limit	The (maximum) configured bitrate limit for the scope during the time interval, or -1 if no limit was configured (kbps).
Bandwidth Limit	The (maximum) configured bandwidth limit for the scope during the time interval, or -1 if no limit was configured (kbps).
Bandwidth Usage	The (maximum) used bandwidth for the scope during the time interval (kbps).
Bandwidth Usage %	The (maximum) percentage of the bandwidth limit used for the scope during the time interval (kbps).
Packet Loss %	Mean packet loss percentage of all QoS reports in the scope during the time interval.
Avg Video Jitter	Mean jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Max Video Jitter	Maximum jitter of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Avg Video Delay	Mean delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Max Video Delay	Maximum delay of all QoS reports of all video channels in the scope during the time interval (milliseconds).
Avg Audio Jitter	Mean jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Max Audio Jitter	Maximum jitter of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Avg Audio Delay	Mean delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Max Audio Delay	Maximum delay of all QoS reports of all audio channels in the scope during the time interval (milliseconds).
Gold Calls	Max concurrent Gold class calls in the scope during the time interval.
Silver Calls	Max concurrent Silver class calls in the scope during the time interval.
Bronze Calls	Max concurrent Bronze class calls in the scope during the time interval.
Audio Calls	Max concurrent audio calls in the scope during the time interval.
Calls 256kbps	Max concurrent video calls with a bitrate less than or equal to 320kbps in the scope during the time interval.
Calls 384kbps	Max concurrent video calls with a bit rate greater than 320kbps and less than or equal to 448kbps in the scope during the time interval.
Calls 512kbps	Max concurrent video calls with a bit rate greater than 448kbps and less than or equal to 640kbps in the scope during the time interval.

**Table 14-14** Network Usage record layout (continued)

Field	Description
Calls 768kbps	Max concurrent video calls with a bit rate greater than 640kbps and less than or equal to 896kbps in the scope during the time interval.
Calls 1Mbps	Max concurrent video calls with a bit rate greater than 896kbps and less than or equal to 1.5Mbps in the scope during the time interval.
Calls 2Mbps	Max concurrent video calls with a bit rate greater than 1.5Mbps and less than or equal to 3Mbps in the scope during the time interval.
Calls 4Mbps	Max concurrent video calls with a bit rate greater than 3Mbps in the scope during the time interval.
SIP Calls	Max concurrent calls using SIP signaling in the scope during the time interval.
H.323 Calls	Max concurrent calls using H.323 signaling in the scope during the time interval.
Gateway Calls	Max concurrent calls using the SIP to H.323 gateway in the scope during the time interval.
Conference Manager Calls	Max concurrent Conference Manager calls in the scope during the time interval.

### To download network usage data

- 1 Go to **Reports > Network Usage**.
- 2 In the **Actions** list, click **Export Network Usage Data**.
- 3 In the **Export Time Frame** dialog box, set the **Start Date** and time and the **End Date** and time you want to include.

The defaults provide all network usage data for the current day.

- 4 Click **OK**.
- 5 Choose a path and filename for the network usage file and click **Save**.

The **File Download** dialog shows the progress.

- 6 When the download is complete, click **Close**.

You can open the CSV file with Microsoft Excel or another spreadsheet application. The file contains a line for each data point.

See also:

[“System Reports”](#) on page 339

[“About Site Topology”](#) on page 241

[“Exporting Network Usage Data”](#) on page 358



# Index

## Symbols

69

## A

- access, system interface 6
- account lockout configuration 50
- activation keys 59
- active calls list 69
- Active Directory 23, 135
  - integration procedure 141
  - integration report 349
  - queries 148
  - settings 137
- add alias dialog 222
- add conference templates dialog 170
- add device authentication dialog 226
- add direct virtual entry queue dialog 192
- add hunt group dialog 221
- add MCU dialog 117
- add MCU pool dialog 128
- add MCU pool order dialog 132
- add MCU zone dialog 207
- add virtual entry queue dialog 191
- adding
  - conference passcodes 146
  - DNS record 18
  - MCU 124
  - second server 333, 334, 335
  - users 267
- alert history 339
- ASCII 5
- associate endpoints with user 275
- audit data 340, 341
- authentication, device 223, 226

## B

- backing up 323
- bandwidth assurance 161
- bandwidth management 203

- banner, login 51
- best practices 291
- bridges 111
- busy out MCU 124

## C

- calendar 153
- calendar service
  - integration procedure 155
- calendar settings 155
- call detail records (CDRs) 344
- call details dialog box 71
- call history 340
- call server
  - capabilities 203
  - configuration 203
- call server overview 2
- call server settings 205
- calls, active 69
- capabilities and constraints, system 4
- cascading, conference 168
- CDR data, export 344
- CDR export history 341, 342
- CDRs 340, 341
- certificate
  - details dialog 34
  - information dialog 32
  - install CA 35
  - install dialog 33
  - install signed 38
  - management list 31
  - overview 27
  - procedures 35
  - remove 39
  - signing request 36
  - signing request dialog 33
- change password dialog 290
- cluster
  - configuration procedures 64
  - settings 53

- clustering 1, 2
- CMA integration 159
- CMA system integration 157
- CMA system page, Polycom 158
- commands, system monitoring 322
- conference
  - cascading 168
  - IVR service 167
  - settings 163
- conference history 341
- conference manager overview 1
- conference manager setup 163
- conference passcodes
  - adding 146
  - enterprise users 146
- conference passwords
  - editing 274
  - enterprise errors report 355
  - export errors data 357
  - local user 271
- conference room
  - errors report 353
  - export errors data 355
  - procedures 282
- conference rooms
  - add or edit 275
- conference templates
  - about 165
  - add dialog 170
  - assigning to enterprise groups 287
  - cascading 168
  - edit dialog 179
  - IVR service 167
  - list 169
  - priority 167
  - procedures 188
  - setting up 24
  - types of 165
  - video frame layout 187
- configuration
  - backup 323
  - call server 203
  - cluster settings 53
  - local user account 50
  - logging 63
  - login sessions 49
  - password requirements 48
  - security 41
  - signaling 20, 60
  - single-server 3
  - site topology 241
  - supercluster 195

- tasks 17
  - two-server cluster 2
- configuration, cluster 64
- connect to enterprise directory 23

## D

- dashboard 296
- dashboard layout 5
- date and time settings 58
- defaults, conference 163
- description, system 1
- details, call 71
- details, certificate 34
- device
  - registration history 348
- device authentication 223
  - add 226
  - edit 226
- device management 69
- devices, registered 73
- dial plan 208
- dial string prefix 60
- dialing prefix 163
- directory, enterprise 23
- DMAs page 196
- DNS record 18
- download
  - CDRs 344
  - enterprise password errors data 357
  - room errors data 355
- dynamic DNS 236

## E

- edit alias dialog 223
- edit conference templates dialog 179
- edit device authentication dialog 226
- edit direct virtual entry queue dialog 193
- edit hunt group dialog 221
- edit MCU dialog 120
- edit MCU pool dialog 129
- edit MCU pool order dialog 133
- edit virtual entry queue dialog 193
- email meeting appointments 153
- endpoint
  - registration history 348
- endpoints
  - associate with user 275
- Endpoints page 73



- enterprise directory 23, 135
    - integration procedure 141
    - integration report 349
    - queries 148
    - settings 137
  - enterprise groups 284, 287
  - enterprise password
    - errors report 355
    - export errors data 357
  - entry queue, direct virtual
    - add 192
  - entry queue, virtual 190
    - add 191
    - edit 193
  - entry queue, virtual direct
    - edit 193
  - errors
    - conference room 353
    - enterprise password 355
  - Exchange Server
    - integration procedure 155
  - Exchange Server integration 153
  - expansion, system 333, 334, 335
  - export
    - CDR data 344
    - enterprise password errors data 357
    - invalid conference rooms data 355
    - network usage data 358
  - export history 341, 342
  - external gatekeepers 82
  - external proxies 88
  - external SBC 106
- F**
- failed server, replacing 336
  - fault tolerance 1, 2
  - field input requirements 5
- G**
- gatekeeper 20, 60
    - internal 203
    - registration history 348
  - gatekeeper settings 205
  - gatekeepers, external 82
  - groups, enterprise 284, 287
  - groups, orphaned 352
- H**
- H.323 prefix 60
  - halting system 337
- hardware
    - replacing 336
    - upgrading 333, 334, 335
  - history
    - alerts 339
    - call 340
    - CDR export 341, 342
    - conference 341
    - retention 238
  - history, registration 348
  - hunt groups 220
    - add 221
    - add alias 222
    - edit 221
    - edit alias 223
- I**
- inactivity lockout 50
  - information, certificate 32
  - initial setup 17
    - add DNS record 18
    - conference templates 24
    - configure signaling 20
    - enterprise directory 23
    - license the system 19
    - MCUs 22
    - security 21
    - testing 25
  - input fields 5
  - install certificates dialog 33
  - integration
    - Active Directory 141
    - CMA 159
    - Exchange Server 153, 155
    - Polycom CMA system 157, 160
    - SRC 161
  - integration report, enterprise directory 349
  - integrations 135
  - interface access 6
  - introduction to system 1
  - invalid conference rooms 353
  - invalid enterprise passwords 355
  - iostat command 323
  - IVR service 167
- J**
- join CMA 159, 160
  - join supercluster dialog 199
  - Juniper Networks SRC 161
  - Juniper Networks SRC integration

- procedure 162
- SRC page 161

## L

- layout, video frame 187
- LDAP 23, 135, 137, 141
- leave CMA 160
- license the system 19
- licenses
  - open source software 9
  - system 59
- logging configuration 63
- login banner 51
- login failure, settings 50
- login policy settings 48
- login sessions 289
- login sessions, settings 49
- logs, system 319

## M

- maintenance
  - overview 291
  - recommended 293
- management
  - certificate 31
  - device 69
  - MCU 111
  - overview 291
  - system 291
  - users and groups 265
- MCU
  - add dialog 117
  - edit dialog 120
  - list 111
  - management 111
  - procedures 124
  - setting up 22
- MCU pool orders
  - add 132
  - edit 133
  - list 130
  - procedures 133
- MCU pools
  - add 128
  - edit 129
  - list 127
  - procedures 129
- MCU zone orders
  - See MCU pool orders*
- MCU zones
  - add dialog 207

- See MCU pools*
- media servers 111
- meeting appointments, Outlook 153
- Microsoft Active Directory 135
- Microsoft Active Directory page 137
- Microsoft Exchange Server page 155
- monitoring the system 296

## N

- network routing rules 57
- network settings 54
- network usage 358
  - export 358
  - exporting data 358
- node
  - adding 333, 334, 335
  - replacing 336
- NTP servers 58

## O

- open ports 4
- open source software 9
- operations
  - system 291
  - users and groups 265
- orphaned groups and users 352
- other systems, integration with 135
- Outlook add-in 153
- overview
  - call server 2
  - capabilities and constraints 4
  - conference manager 1
  - management and maintenance 291
  - superclustering 3
  - system 1

## P

- packages, open source software 9
- passcodes, conference
  - enterprise users 146
- password requirements, local 48
- password, local user
  - change dialog 290
- passwords, conference
  - editing 274
  - enterprise errors report 355
  - export errors data 357
  - local user 271
- permissions, user 265

- ping command 322
  - Polycom CMA system
    - integration 157
    - procedures 160
  - Polycom CMA system page 158
  - Polycom Conferencing meetings 153
  - pool orders, MCU
    - add 132
    - edit 133
    - list 130
    - procedures 133
  - pools, MCU
    - add 128
    - edit 129
    - list 127
    - procedures 129
  - port usage 4
  - postliminary scripts, sample 216
  - prefix service 234
  - prefix, dialing 163
  - preliminary scripts, sample 216
  - priority, template 167
  - procedures
    - cluster configuration 64
    - site topology 263
  - professional services 5
  - profiles, RMX 165
  - proxies, external 88
- Q**
- QoS statistics
    - network usage 358
    - site 81
    - site link 82
  - queries, Active Directory 148
- R**
- record retention, history 238
  - records
    - call 340
    - CDR exports 341, 342
    - conference 341
  - redundancy 1, 2
  - registered devices 73
  - registration history 348
  - regular maintenance tasks 293
  - replacing failed server 336
  - report
    - registration history 348
  - reports 339
    - active calls 69
    - alert history 339
    - call history 340, 341, 342
    - conference history 341
    - conference room errors 353
    - enterprise directory integration 349
    - enterprise password errors 355
    - network usage 358
    - orphaned groups and users 352
  - restarting system 337
  - restoring from backup 323
  - RMX
    - devices 111
    - profiles 165
  - roles, user
    - and system access 6
    - assigning to enterprise groups 287
    - overview 265
  - room errors data, export 355
  - routing configuration 57
- S**
- s elect layout dialog 187
  - sample scripts 216
  - sar command 323
  - SBC, external 106
  - scripts, preliminary and postliminary 216
  - security
    - certificate procedures 35
    - configuration settings 41
    - overview 27
    - system 27
  - security, setting up 21
  - server
    - adding 333, 334, 335
    - replacing 336
    - settings 53
  - session and resource controller (SRC) 161
  - session configuration 49
  - sessions, login 289
  - set up
    - conference templates 24
    - MCUs 22
    - security 21
  - settings
    - Active Directory integration 137
    - calendar 155
    - cluster 53
    - conference 163
    - history retention 238

- logging 63
- network 54
- signaling 60
- time 58
- settings dialog 5
- setup
  - conference manager 163
  - initial 17
  - supercluster 196
  - testing 25
- shared number dialing 190
  - add direct VEQ 192
  - add VEQ 191
  - edit direct VEQ 193
  - edit VEQ 193
- shutting down 337
- signaling configuration 60
- signaling, configuring 20
- signed certificate
  - install 38
  - remove 39
- signing request, certificate 33
- single-server configuration 3
- SIP proxy 203
- SIP proxy settings 205
- site
  - statistics 81
- site link
  - statistics 82
- site topology 241
  - from CMA 159
  - from CMA system 157
  - procedures 263
- software
  - licenses 59
  - open source packages 9
  - upgrade procedures 330
  - upgrading 328
- solution support 5
- SRC
  - integration 161
- SRC integration
  - Juniper Networks SRC page 161
  - procedure 162
- statistics
  - network usage 358
  - site 81
  - site link 82
- status, system 296, 322
- supercluster
  - about 195

- call server settings 205
- join dialog 199
- procedures 200
- setup 196
- upgrading 329
- supercluster configuration 195
- superclustering overview 3
- support 5
- system
  - capabilities and constraints 4
  - cluster settings 53
  - configuration procedures 64
  - dashboard 296
  - initial configuration summary 17
  - introduction 1
  - license 19
  - logs 319
  - maintaining 293
  - operations 291
  - overview 1
  - reports 339
  - security 27
  - testing 25
  - time 58
  - views 6
  - working in 5

## T

- templates, conference
  - about 165
  - add dialog 170
  - assigning to enterprise groups 287
  - cascading 168
  - edit dialog 179
  - IVR service 167
  - list 169
  - priority 167
  - procedures 188
  - setting up 24
  - types of 165
  - video frame layout 187
- testing initial setup 25
- text size 5
- time settings 58
- tools, system management 322
- top command 322
- topology, site 241, 263
- traceroute command 322
- Trusted Root CA
  - install 35
  - remove 39
- two-server configuration 2

**U**

- Unicode 5
- upgrading
  - hardware 333, 334, 335
  - procedures 330
  - software 328
  - supercluster 329
- user
  - associate endpoints 275
  - conference rooms 275
- user groups 284, 287
- user roles
  - and system access 6
  - assigning to enterprise groups 287
  - overview 265
- user sessions, monitoring 289
- users
  - adding 267
  - password requirements, local 48
  - procedures 280
- users and groups 265
- users page 268
- users, orphaned 352

**V**

- version upgrade 328
- Video Border Proxy 106
- video frame layout 187
- virtual entry queue 190
  - add 191
  - edit 193
- virtual entry queue, direct
  - add 192
  - edit 193

**W**

- working in system 5

**X**

- X.509 certificates 27

**Z**

- zone orders, MCU
  - See pool orders, MCU*
- zones, MCU
  - See pools, MCU*

