POLYCOM®

▶ Polycom® DMA™ 7000 System
Operations Guide

5.1 | November 2012 | 3725-76302-001L1

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.

Contents

1

Polycom® DMA™ 7000 System Overview

This chapter provides an overview of the Polycom® Distributed Media Application™ (DMA™) 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® Proxias™ application server. The following topics introduce you to the system:

- The Polycom DMA System's Primary Functions
- The Polycom DMA System's Three Configurations
- System Capabilities and Constraints
- System Port Usage

The Polycom DMA System's Primary Functions

Conference Manager

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® Active Directory®, automating the task of provisioning users with virtual meeting rooms (VMRs) 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

The Polycom DMA system's Call Server provides the following functionality:

* H.323 gatekeeper

* SIP registrar and proxy server

* XMPP server (client-to-client connectivity, including chat and presence information, for clients logged into the server)

* H.323 <—> SIP transition gateway

* Dial plan and prefix services

* Device authentication

- Bandwidth management

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

RealPresence Platform API

This version of the Polycom DMA system optionally allows an API client application, developed by you or a third party, to access the RealPresence Platform Application Programming Interface (API). This API access is licensed separately. It provides programmatic access to the Polycom DMA system for the following:

- Provisioning

- Conference control and monitoring

- Call control and dial-out

- Billing and usage data retrieval

- Resource availability queries

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

No separate license is needed in order for a Polycom RealPresence Resource Manager system to integrate with the DMA system via the API. This integration provides the full programmatic access to the DMA system described above, and enables users of the RealPresence Resource Manager scheduling interface to:

- Schedule conferences using the DMA system's MCU resources.

- Set up *Anytime* conferences. Anytime conferences are referred to as *preset dial-out* conferences in the DMA system (see "Edit Conference Room Dialog Box" on page 329)

Note

Integrating the Polycom RealPresence Resource Manager system with the DMA system via the API is separate and distinct from integrating the DMA system with a Polycom CMA or RealPresence Resource Manager system.

- The former enables RealPresence Resource Manager users to obtain information from and use functionality of the DMA system that would otherwise be accessible only in the DMA system's management interface.
- The latter enables the DMA system to retrieve site topology and user-to-device associations from the CMA or RealPresence Resource Manager system.

For convenience, however, when you perform the former operation, the latter integration is automatically performed for you so that the DMA system will have the site topology and user-to-device information that the RealPresence Resource Manager system expects it to have.

SVC Conferencing Support

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

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

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

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

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

• Improved video quality at lower bandwidths

• Improved audio and video error resiliency (good audio quality with more than 50% packet loss, good video quality with more than 25% packet loss)

• Lower end-to-end latency (typically less than half that of AVC)

• More efficient use of bandwidth

• Lower infrastructure cost and operational expenses

• Easier to provision, control, and monitor

• Better security (end-to-end encryption)

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

See also:

The Polycom DMA System's Three Configurations

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 or reconnected to the point-to-point call they were in. 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 server 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 and better network traffic management, up to five geographically distributed Polycom DMA system clusters (two-server or single-server) can be integrated into a *supercluster*. All five clusters can be Call Servers (function as gatekeeper, SIP proxy, SIP registrar, and gateway). Up to three can be designated as Conference Managers (manage an MCU resource pool to host conference rooms).

The superclustered 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-server 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.
>
> It's important to understand the difference between two co-located servers forming a single DMA system (cluster) and two geographically distributed DMA clusters (single-server or two-server) joined into a supercluster.
>
> A single two-server DMA system (cluster) has the following characteristics:
>
> - A single shared virtual IP address and FQDN, which switches from one server to the other when necessary to provide local redundancy and fault tolerance.
> - A single management interface and set of local settings.
> - Ability to manage a single territory, with no territory management backup.
> - A single set of Call Server and Conference Manager responsibilities.
>
> A supercluster consisting of two DMA clusters (single-server or two-server) has the following characteristics:
>
> - Separate IP addresses and FQDNs for each cluster.
> - Separate management interfaces and sets of local settings for each cluster.
> - Ability for each cluster to manage its own territory, with another cluster able to serve as backup for that territory.
> - Different Call Server and Conference Manager responsibilities for each territory and thus each cluster.

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 RealPresence Resource Manager or CMA system)
- Number of MCUs enabled for conference rooms: 64
- Number of territories enabled for conference rooms (Conference Manager enabled): 3
- Number of concurrent VMR calls: 1200 per territory (Conference Manager), up to 3600 total
- Size of Active Directory supported: 1,000,000 users and 1,000,000 groups (up to 10,000 groups may be imported)

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

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

System Port Usage

The table below lists the inbound ports that may be open on the Polycom DMA system, depending on signaling and security settings, integrations, and system configuration.

Table 1-1   *Inbound port usage*

Port	Protocol	Description
22	TCP	SSH. Only available if Linux console access is enabled (see "Security Settings" on page 48).
80	TCP	HTTP. Redirects to 443 (HTTP access is not allowed). Disabled in maximum security mode.
443	TCP	HTTPS. Redirects to 8443.
1718	UDP	H.323 RAS. Default port; can be changed (see "Signaling Settings" on page 71).

Table 1-1   *Inbound port usage (continued)*

Port	Protocol	Description
1719	UDP	H.323 RAS. Default port; can be changed (see "Signaling Settings" on page 71).
1720	TCP	H.323 H.225 signaling. Default port; can be changed (see "Signaling Settings" on page 71).
1935	TCP/UDP	XMPP. Traditional RTMP, Flash communication server.
1936	TCP/UDP	XMPP. Flash communication server.
4449	TCP	LDAP. OpenDJ replication (superclustering).
5060	TCP/UDP	Unencrypted SIP. Default port; can be changed or disabled (see "Signaling Settings" on page 71).
5061	TCP	SIP TLS. Default port; can be changed (see "Signaling Settings" on page 71).
5080	TCP/UDP	XMPP. Tomcat or jetty servlet container.
5222	TCP	Unencrypted XMPP. Default port; can be changed or disabled (see "Signaling Settings" on page 71).
5223	TCP	XMPP TLS. Default port; can be changed (see "Signaling Settings" on page 71).
5269	TCP/UDP	XMPP. Server to server communications for federation.
7070	TCP	XMPP HTTP connections.
8088	TCP	XMPP. Traditional RTMP tunneled over HTTP.
8443	TCP	HTTPS. Management interface access.
8444	TCP	HTTPS. Supercluster communication.
8989	TCP	LDAP. OpenDJ replication (superclustering).
9090	TCP	HTTPS. Upgrade status monitoring (only while upgrade process is running). XMPP server administration console.
36000-61000	TCP	H.323 H.245 port range.

The table below lists the remote ports to which the Polycom DMA system may connect, depending on signaling and security settings, integrations, and system configuration.

Table 1-2   *Outbound port usage*

Port	Protocol	Description
80	TCP	HTTP. MCUs, Exchange Web Services (calendaring). Only available if unencrypted connections are enabled (see "Security Settings" on page 48).
389	TCP	LDAP. Active Directory integration.
443	TCP	HTTPS. MCUs, Exchange Web Services (calendaring).
389	TCP	LDAP. Active Directory integration.
1718	UDP	H.323 RAS. Default port; can be changed (see "Signaling Settings" on page 71).
1719	UDP	H.323 RAS. Default port; can be changed (see "Signaling Settings" on page 71).
1720	TCP	H.323 H.225 signaling. Default port; can be changed (see "Signaling Settings" on page 71).
3268	TCP	Global Catalog. Active Directory integration.
3269	TCP	Secure Global Catalog. Active Directory integration.
4449	TCP	OpenDJ replication (superclustering).
5060	TCP/UDP	Unencrypted SIP. Default port; can be changed or disabled (see "Signaling Settings" on page 71).
5061	TCP	SIP TLS. Default port; can be changed (see "Signaling Settings" on page 71).
8443	TCP	HTTPS. Management interface access.
8444	TCP	Supercluster communication.
8989	TCP	OpenDJ replication (superclustering).
36000-61000	TCP	H.323 H.245 port range.
32768-61000	TCP/UDP	XMPP. Ephemeral 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 visit www.polycom.com/services/professional_services/ 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.

Accessing the Polycom DMA System

The Polycom DMA system's management interface is accessed by pointing a compatible browser equipped with Adobe® Flash® Player to the system's host name or IP address (a two-server cluster or an IPv6-only single-server cluster has a virtual host name and IP address, and we strongly recommend always using the virtual address). Minimum requirements:

- Microsoft Internet Explorer® 7 or newer, or Mozilla Firefox® 3 or newer, or Google Chrome 11 or newer

- Adobe Flash Player 9.0.124 or newer

- 1280x1024 minimum display resolution (1680x1050 or greater recommended)

> **Note**
>
> The Polycom DMA system's Flex-based management interface requires Adobe Flash Player. For stability and security reasons, we recommend always using the latest version of Flash Player.
>
> Even so, be aware that your browser's Flash plugin may hang or crash from time to time. Your browser should alert you when this happens and enable you to reload the plugin. In some cases, you may need to close and restart your browser.
>
> In the Google Chrome browser, use the Adobe Flash plugin, not the built-in Flash support.

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 [icon] 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 User Roles and Their Access Privileges

The Polycom DMA system has three system user roles (see "User Roles Overview" on page 312) that provide access to the management and operations interface and, if available, the separately licensed RealPresence Platform Application Programming Interface (API). The functions you can perform and parts of the interface or API resources you can access depend on your user role or roles, as shown in the tables below.

Table 1-3   *Management interface access privileges*

Menu/Icon	Admin	Provisioner	Auditor
[icon] Home. Returns to the Dashboard.	●	●	●
Network >			
Active Calls	●	●	
Endpoints	●	●	
DMAs [1]	●	●	

Table 1-3   *Management interface access privileges*

Menu/Icon	Admin	Provisioner	Auditor
MCU > MCUs [1]	●	●	
MCU > MCU Pools [1]	●	●	
MCU > MCU Pool Orders [1]	●	●	
Site Statistics [1]	●	●	
Site Link Statistics [1]	●	●	
Site Topology > Sites [1]	●	●	
Site Topology > Site Links [1]	●	●	
Site Topology > Site-to-Site Exclusions [1]	●	●	
Site Topology > Network Clouds [1]	●	●	
Site Topology > Territories [1]	●	●	
External Gatekeeper [1]	●	●	
External SIP Peer [1]	●	●	
External SBC [1]	●	●	
User >			
Users [2]	●	●	
Groups	●		
Login Sessions [1]	●	●	
Change Password	●	●	●
Reports >			
Call History	●	●	●
Conference History	●	●	●
Registration History	●	●	●
Network Usage	●	●	
Microsoft Active Directory Integration [3]	●		
Enterprise Passcode Errors [3]	●		
Orphaned Groups and Users	●	●	
Conference Room Errors [3]	●		

Table 1-3   *Management interface access privileges*

Menu/Icon	Admin	Provisioner	Auditor
Maintenance			
System Log Files [4]	●		●
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 [1]	●	●	
Embedded DNS	●		
History Retention Settings	●		●
Admin > Integrations >			
Microsoft Active Directory	●		
Microsoft Exchange Server	●		
Polycom RealPresence Resource Manager or CMA System	●		
Juniper Networks SRC	●		

Table 1-3   *Management interface access privileges*

Menu/Icon	Admin	Provisioner	Auditor
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.	●	●	●

1. Provisioners have view-only access.
2. 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.
3. Must be an enterprise user to view this report.
4. Administrators can't delete log archives.

Table 1-4 *API resource access privileges*

API Resource	Admin	Provisioner	Auditor	Conference Room Owner
user[1][2]	●	●		●
conference-room[1][2]	●	●		●
conference-template[3]	●	●		
billing	●	●	●	
conference[1]	●	●		●
participant[1]	●	●		●
conference-observer[1]	●	●		●
participant-observer[1]	●	●		
mcu	●	●		
mcu-pool	●	●		
mcu-pool-order	●	●		
territory	●	●		
call-server-configuration	●		●	
device	●	●		
device-observer	●	●		
group	●	●		
status	●	●	●	
subscription[1]	●	●		●
user-role	●	●		

1. Conference Room Owners can only access resources that they own and can't use PUT, POST, or DELETE methods on their user account or conference rooms.

2. Provisioners can't add or remove roles or associated endpoints, and can't edit user accounts with explicitly assigned roles (Administrator, Provisioner, or Auditor), but can manage their conference rooms.

3. Provisioners can GET a list of conference templates, but can't GET a specific conference template.

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. Note that although you're free to modify the LGPL modules used in the Polycom DMA system in any way you wish, we cannot be responsible if the changes you make impair the 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 **Admin > Local Cluster > 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	http://www.apache.org/licenses/LICENSE-2.0
bsf	2.3.0-rc1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
CentOs	5.8	GPLv2 and multiple others	https:/www.redhat.com/licenses/gpl.html
cxf	2.4.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
Cluster-glue	1.0.5	GPLv2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
commons-beanutils	1.7	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-collections	3.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-configuration	1.5	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-digester	1.6	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-discovery	0.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-fileupload	1.2.1	Apache License, Version 2	http://commons.apache.org/fileupload/license.html
commons-httpclient	3.0.1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-io	1.4	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-jexl	1.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-jxpath	1.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-lang	2.3	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-logging	1.0.4	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-pool	1.3	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
corosync	1.2.5	BSD	http://opensource.org/licenses/bsd-license.php

Software	Version	License	Link
dom4j	1.5.2	BSD-style	http://www.dom4j.org/license.html
drools	4.0.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
Hibernate Annotations	4.2.1.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Hibernate (core)	3.2.4 SP 1	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Hsqldb	2.0.1-rc1	BSD-style	http://hsqldb.org/web/hsqlLicense.html
JAF	1.1	Oracle Corporation Binary Code License Agreement	http://www.oracle.com/technetwork/java/javase/downloads/java-se-archive-license-1382604.html
jamon	2.2	BSD-style	http://jamonapi.sourceforge.net/#JAMonLicense
Java JRE	1.7.0.9	Oracle Corporation Binary Code License Agreement	http://www.java.com/en/download/license.jsp
JavaMail	1.4	Oracle Corporation Binary Code License Agreement	http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-eeplat-419426.html#javamail-1.4-oth-JPR
jaxb2-basics-runtime	0.6.0	BSD-style	http://confluence.highsource.org/display/J2B/License
JBOSS AS	4.2.1 GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-aop	1.5.5	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-cache	1.4.1.sp14	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-jaxws	2.0.0.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-jmx	4.2.1.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-remoting	2.2.2.sp1	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-serialization	4.2.1.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jgroups	2.4.8.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
jcifs	1.3.2	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
jna	3.0.9 b0	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
joesnmp	0.3.4	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
jsr311-api	1.1.1	CDDL	http://www.opensource.org/licenses/cddl1.php
libesmtp	1.0.4	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html

Software	Version	License	Link
libnet	1.1.4		
libxml2	1.2.3	MIT License	http://www.opensource.org/licenses/mit-license.html
Log4j	1.2.14	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
neethi	3.0.1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
NSS	Part of Centos distrib.	Mozilla Public License v1.1	http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1
NSS Tools	Part of Centos distrib.	Mozilla Public License v1.1	http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1
NTP	Part of Centos distrib.	Open Software License v3.0	http://www.opensource.org/licenses/ntp-license.php
OpenDJ	2.5.0	CDDL-1.0	http://www.opensource.org/licenses/cddl1.php
openSSH	Part of Centos distrib.	OpenSSH	http://www.openssh.org
openSSL	Part of Centos distrib.	OpenSSL	http://www.openssl.org/source/license.html
Python	Part of Centos distrib.	Python Software Foundation License Version 2	http://python.org/download/releases/2.6.2/license
Quartz	1.5.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
sudo	1.7.2p1	ISCL	https://www.isc.org/software/license
Xerces2	See JBoss.	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
OpenFire		Apache License, Version 2	http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html
Rhino		Mozilla Public License, v1.1	http://www.mozilla.org/MPL/MPL-1.1.html AND https://developer.mozilla.org/en/Rhino_License

Software	Version	License	Link
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.	http://creativecommons.org/licenses/by-nc-sa/3.0/ http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html
xmlschema-core	2.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
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 http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT			
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])	

Software	Version	License	Link
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)	
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)	

Software	Version	License	Link
RelaxNGCC		(general permissive)	
RELAX NG Object Model/ Parser		MIT License	
XFree86-VidMode Extension		Version 1.1 of Project Licence (BSD-like)	
RelaxNGCC		version 2003-May-08 of the Info-ZIP copyright and license	ftp://ftp.info-zip.org/pub/infozip/license.html
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)	

2

Polycom® DMA™ System Initial Configuration Summary

This chapter describes the configuration tasks required to complete your implementation of a new Polycom® Distributed Media Application™ (DMA™) 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), 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 and Optionally Create a Supercluster

- 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 198).
- Configure calendaring service ("Microsoft Exchange Server Integration" on page 180).

Add Required DNS Records for the Polycom DMA System

Note

If you're not familiar with DNS administration, the creation of various kinds of DNS resource records (A/AAAA,NAPTR, NS, and SRV), your enterprise's DNS implementation, and tuning for load balancing (if needed), please consult with someone who is.

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 (address) resource record (RR) 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. This address is shared between the servers in a two-server cluster configuration. For administrative convenience, we recommend that you also create alias records for the physical host name(s) and IP address(es). For a superclustered system, A/AAAA records for each physical host name, physical IP address, virtual host name, and virtual IP address 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.

The DNS server(s) should also have entries for your Microsoft® Active Directory® server (if different from the DNS server) and any external gatekeepers or SIP peers.

You may need 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 and ease future network administrative burdens, create the following DNS records (for each cluster in a supercluster, if applicable):

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

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

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

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

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

Additional DNS Records for H.323 Gatekeeper

To support the use of your Polycom DMA system as an H.323 gatekeeper and ease future network administrative burdens, create SRV records that 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. Here are example records for two clusters:

```
_h323ls._udp.example.com.  86400 IN SRV 0 1 1719 dma-asia.example.com.
_h323ls._udp.example.com.  86400 IN SRV 0 1 1719 dma-europe.example.com.
_h323cs._tcp.example.com.  86400 IN SRV 0 1 1720 dma-asia.example.com.
_h323cs._tcp.example.com.  86400 IN SRV 0 1 1720 dma-europe.example.com.
```

To enable access from the public internet, create corresponding SRV records, visible from outside the firewall, for the public address of each H.323 session border controller (SBC).

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

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 279), 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 name. Here are example records for two clusters:

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

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

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

Verify That DNS Is Working for All Addresses

To confirm that DNS can resolve all the host names and/or FQDNs, ping each of them, either from a command prompt on the PC you're using to access the system or from one of the clusters you're setting up (go to **Troubleshooting Utilities > Ping**).

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

License the Polycom DMA System

A Polycom DMA system is licensed at the cluster level (single-server or two-server). A cluster's license specifies:

• The maximum number of concurrent calls that can touch the cluster. In a supercluster configuration, note that:

— A single call may touch more than one cluster. It consumes a license on each cluster it touches.

— Each cluster may be licensed for a different number of calls.

— If your superclustering strategy (see "About Superclustering" on page 227) calls for a cluster to be primary for one territory and backup for another, it must be licensed for the call volume expected when it has to take over the territory for which it's the backup.

- Whether the RealPresence Platform Application Programming Interface (API) is enabled. The API provides an API client application with programmatic access to the Polycom DMA system (see "RealPresence Platform API" on page 3). In a supercluster, all clusters must have the same API licensing status.

> **Note**
>
> An API license isn't required in order for a Polycom RealPresence Resource Manager system to access the API. It's only needed for a client application you or a third party develop.

You should have received either one or two license numbers for each cluster, depending on whether you ordered a single-server or 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 70.

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 83.

Configure the Call Server and Optionally Create a Supercluster

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

1   Integrate with a Polycom RealPresence Resource Manager or CMA system (see "Resource Management System Integration" on page 185) or enter site topology information (see "Site Topology" on page 283).

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 48). But wait until after superclustering to do the rest of the security setup tasks.

    b   Depending on security settings, you may need to install certificates before superclustering (see "Certificate Procedures" on page 42).

    c   Create a supercluster (see "About Superclustering" on page 227) and configure supercluster options.

3   Create territories and assign sites to them (if you integrated with a Polycom RealPresence Resource Manager or CMA system, this must be done on that system). Assign the primary and backup cluster responsible for each territory, and designate which territories can host conference rooms (see "Territories" on page 302).

4   Add any external devices, such as a neighbor gatekeeper or SIP peer (see "Call Server Configuration" on page 237).

5   Configure the dial plan (see "Dial Rules" on page 243).

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 other 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 313 and "Users Procedures" on page 333.

2   Create the Active Directory 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 169.

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 312) from the service account used to integrate with Active Directory. See "Connect to Microsoft Active Directory" on page 32 and "Microsoft Active Directory Integration" on page 163.

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 163, "Users Procedures" on page 333, and "Conference Room Errors Report" on page 422.

6   Obtain and install a security certificate from a trusted certificate authority. See "Security Certificates Overview" on page 35 and "Certificate Procedures" on page 42.

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 381.

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 and Optionally Create a Supercluster" on page 28 and "About Superclustering" on page 227), 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 and Optionally Create a Supercluster" on page 28.

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 131.

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.

> **Note**
>
> If you have a Polycom RealPresence Resource Manager system that's going to use the DMA system API to schedule conferences on the DMA system's conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for the use of the RealPresence Resource Manager system. The pool orders should be named in such a way that:
>
> • They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
>
> • Users of that system will understand that they should choose one of those pool orders.
>
> If the RealPresence Resource Manager system is also going to be used to directly schedule conferences on MCUs, those MCUs should not be part of the conferencing resources (MCU pools) available to the DMA system.

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 152 and "MCU Pool Orders" on page 156 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 195).

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 163.

> **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 64.

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 and Optionally Create a Supercluster" on page 28) 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, or VMR). The conference room IDs are typically generated from the enterprise users' phone numbers.

> **Note**
>
> Creating conference rooms 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 335.

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 certain 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 (for instance, for management interface login); 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 195). They can also have their own MCU pool order, which preferentially routes conferences to certain MCUs (see "MCU Pool Orders" on page 156).

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 312, "Groups" on page 338, and "Enterprise Groups Procedures" on page 342.

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 28.

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 220. To change conference settings, see "Conference Settings" on page 193. To customize the conferencing experience for an enterprise group, see "Enterprise Groups Procedures" on page 342.

Test the System

On the **Signaling Settings** page (see "Signaling Settings" on page 71), 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 352), 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 381.

3

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: • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Sometimes intermediate certificates. Upload file or paste into text box.
	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: • A signed certificate for the system, authenticating its public key. • A private key for the system. • The CA's public certificate. Upload file.
	PKCS #7 protocol P7B file	Certificate chain containing: • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Sometimes intermediate certificates. Upload file.
	CER (single certificate) file	Signed certificate for the system, authenticating its public key. Upload file.

How Certificates Are Used by the Polycom DMA System

The Polycom DMA system uses X.509 certificates in the following 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 42).

    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 180), 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 48), 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 352) 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).

5   When performing call signaling requiring TLS, the Polycom DMA system presents its certificate to the connecting client (one-way TLS). Unless the **Skip certificate validation for encrypted signaling** security option is enabled (see "Security Settings" on page 48), the system uses the installed CA certificates to authenticate the connecting client's certificate as well (mTLS or two-way TLS).

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. Alternatively, if the certificate you want to reinstall is a PKCS#12 certificate, it contains a private key and will replace both the public key and the private key generated at installation time.

See also:

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

See also:

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 **Network** 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:

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:

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 **Password** field and **Upload file** 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:

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 35

"Certificate Settings" on page 38

"Certificate Procedures" on page 42

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:

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. This method uses the private key generated at software installation time.

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.

  b   In the **Actions** list, select **Display Details**.

    The Certificate Details dialog box appears. If this is the default self-signed certificate, **Organizational Unit** is *Self Signed Certificate*.

  c   To close the dialog box, click **OK**.

3   In the **Actions** list, select **Create Certificate Signing Request**.

  If you've created a signing request before, you're asked if you want to use your existing certificate request or generate a new one. Elect to generate a new one.

4 In the **Certificate Information** dialog box, enter the identifying information for your Polycom DMA system (see "Certificate Information Dialog Box" on page 40) and click **OK**.

The **Certificate Signing Request** dialog box displays the encoded request (see "Certificate Signing Request Dialog Box" on page 40).

5 Copy the entire contents of the **Encoded Request** box (including the text `-----BEGIN NEW CERTIFICATE REQUEST-----` and `-----END NEW CERTIFICATE REQUEST-----`) and submit it to your certificate authority.

Depending on the certificate authority, your CSR may be submitted via email or by pasting into a web page.

6 Click **OK** to close the dialog box.

When your certificate authority has processed your request, it sends you a signed public certificate for your Polycom DMA system. Some certificate authorities also send intermediate certificates and/or root certificates. Depending on the certificate authority, these certificates may arrive as email text, email attachments, or be available on a secure web page.

The Polycom DMA system accepts PKCS#7 or PKCS#12 certificate chains or single certificates.

Caution

When you submit the CSR to your CA, make sure that the CA doesn't modify any of the predefined SAN fields or the X.509v3 Key Usage or Extended Key Usage fields. Changes to these fields may make your system unusable. Contact Polycom technical support if you have any questions about this.

See also:

"Security Certificates Overview" on page 35

"Certificate Settings" on page 38

"Certificate Procedures" on page 42

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:

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 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 54). 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
Maximum security	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.
High security	Recommended setting for normal operation.
Custom security	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	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. This configuration causes an extreme security flaw: the unencrypted passwords of enterprise users are transmitted over the network, where they can easily be intercepted. 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.
Allow unencrypted connections to MCUs	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. 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.
Allow unencrypted calendar notifications from Exchange server	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. If this option is selected, the Polycom DMA system does not require HTTPS for calendar notifications. We recommend installing a certificate trusted by the Exchange server and using an HTTPS URL for notifications rather than enabling this option.

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

Field	Description
Allow basic authentication to Exchange server	Normally, if calendaring is enabled, the Polycom DMA system authenticates itself with the Exchange server using NTLM authentication.
	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).
	We recommend using NTLM authentication rather than enabling this option.
	In order for either NTLM or HTTP Basic authentication to work, they must be enabled on the Exchange server.
Skip certificate validation for server connecting	Normally, when the Polycom DMA system connects to a server, it validates that server's certificate.
	This option configures the system to accept any certificate presented to it without validating it.
	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:

	MCUs
	    Active Directory
	    Exchange
	    RealPresence Resource Manager or CMA system
	    Other DMA systems

Skip certificate validation for encrypted signaling	Normally, during encrypted call signaling (SIP over TLS), the Polycom DMA system requires the remote party (endpoint or MCU) to present a valid certificate. This is known as mTLS or two-way TLS.
	This option configures the system to accept any certificate (or none).
	We recommend installing valid certificates on your endpoints and MCUs rather than enabling this option.

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

Field	Description
Skip certificate validation for user login sessions	This option may be configured in any security mode.
	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 (this is known as mTLS for administrative connections).
	Turn this option off only if:
	• 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.
	• The CA's public certificate is installed in the Polycom DMA system so that it trusts the CA.
	• All authorized users, including yourself, have a client certificate signed by the CA that authenticates them to the Polycom DMA system.
Allow forwarding of IPv6 ICMP destination unreachable messages	If this option is off, the Polycom DMA system has an internal firewall rule that blocks outbound destination unreachable messages.
	If this option is on, that firewall rule is disabled.
	Note: The Polycom DMA system currently doesn't send such messages, regardless of this setting.
Allow IPv6 ICMP echo reply messages to multicast addresses	If this option is off, the Polycom DMA system doesn't reply to echo request messages sent to multicast addresses (multicast pings).
	If this option is on, the system responds to multicast pings.

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

Field	Description
Disable enhanced support	Enhanced support allows Polycom Global Services personnel to securely access the system when normal access methods aren't possible. For example, enhanced support could allow support of a DMA system when console access is disabled and system errors prevent access to the management interface.
	Using the enhanced support feature, expert Polycom Global Services personnel can enable console access when necessary using Single Packet Authorization (SPA) technology. This is a more secure method than console access, so the default is to not disable it.
	We strongly recommend leaving this setting off so that the enhanced support feature remains available. If neither enhanced support nor console access is available, recovering from a serious problem may require re-imaging the system, resulting in a loss of data.
	This setting is automatically turned on if **Maximum security** is enabled.

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:

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, and the enhanced support feature is 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.

- SIP signaling is not supported.

- Superclustering is not supported.

- 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 RealPresence Resource Manager or CMA system is not supported.

- On the **Banner** page, **Enable login banner** is selected and can't be disabled.

- On the **Login Sessions** page, the **Terminate Session** action is not available.

- On the **Troubleshooting Utilities** 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 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).

- 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.

  Each enterprise user can have only one assigned role (Administrator, Provisioner, or Auditor). If some enterprise users have multiple roles (or inherit multiple roles from their group memberships), they retain only the lowest-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:

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:

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
Password Management	
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).
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).
Password Complexity	
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 35

"Login Policy Settings" on page 57

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 344.

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 **Unlimited**.
	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 **Unlimited**.
Session timeout (minutes)	Specify the length of time after which the system terminates a session for inactivity or select **Unlimited**.

See also:

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
Account Lockout	
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.
Account Inactivity	
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 35

"Login Policy Settings" on page 57

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 **Message** 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 **Custom** 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 **Message** field, and you can then edit the copy. When you do so, the system resets the list to **Custom**.
	Your edits don't affect the stored sample. You can revert to the original version of the sample by re-selecting it from the list.

See also:

Reset System Passwords

In an extremely high-security environment, security compliance 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:

4

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 23 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 RealPresence Resource Manager or 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 RealPresence Resource Manager or CMA system. See "Superclustering" on page 227 or "Resource Management System Integration" on page 185.

Incorrect network information may make the system unuseable and the management interface unreachable.

Note

This version of the Polycom DMA system eliminates the need for virtual host name(s) and IP addresses in a single-server system or cluster. When a version 5.0 or earlier single-server DMA system is upgraded to version 5.1 or later, the previous version's virtual host name(s) and IP addresses become the upgraded version's physical host name(s) and IP addresses, so accessing the system doesn't change.

(Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.)

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

Field	Description
System IP type	IP addressing supported (IPv4, IPv6, or both).
System server configuration	Number of servers (1 or 2) in this cluster. Caution: Once this is set to **2 server configuration**, it can't be changed back to **1 server configuration**. To reconfigure a two-server system as two separate single-server systems, you must use the USB Configuration Utility. See the *Getting Started Guide*.
System split network setting	Specifies whether management and signaling traffic are combined on one network interface or split onto separate interfaces. **Caution:** Split networking is for network configurations in which signaling and management traffic are not on the same network. To split the network configuration, you must use different gateways and subnets for management and signaling, and separate physical connections for the management and signaling networks (eth0 for management, eth2 for signaling). If management and signaling traffic are combined on the same network (subnet), both use the same physical and virtual IP addresses and the same network interface.
Server 1	Status, host name, and IP address(es) of the primary server. 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.
Server 2	Status, host name and IP address(es) of the secondary server. The fields in this section duplicate those in the Server 1 section and are enabled only in two-server configuration.

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

Field	Description
Shared Management Network Settings	The settings in this section apply to the entire system (both servers in two-server configuration), whether management and signaling are combined or separate.
Virtual host name IPv4 IPv6	Virtual host name and IP address(es) for the system's management (or combined) network interface. For a one-server configuration, these fields are disabled. (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.) 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.
Subnet mask	IPv4 network mask that defines the subnetwork of the system's management interface.
IPv6 prefix length	IPv6 CIDR (Classless Inter-Domain Routing) value that defines the subnetwork of the system's management interface.
IPv4 gateway	IPv4 address of gateway server for the subnetwork.
Name Enable	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.
Auto-negotiation Speed Duplex	Turn on **Auto-negotiation** or set **Speed** and **Duplex** manually.
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.

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

Field	Description
Shared Signaling Network Settings	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 servers in two-server configuration).
	For a one-server configuration, the virtual host name and IP fields are disabled. (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.)
	The settings are the same as those in **Shared Management Network Settings**, 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 servers in a two-server cluster.)
General System Network Settings	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 "Microsoft Active Directory Integration" on page 163.
DNS 2	
DNS 3	
Domain	Fully qualified domain name for the system.

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

Field	Description
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:
	<IPv6_address>%eth0
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:

Routing Configuration Dialog Box

In the **Network** page's action list, the **Routing Configuration** command opens the **Routing Configuration** dialog box, where you can add or delete network routing rules (IPv4, IPv6, or both, depending on the **System IP type** setting on the **Network** page). The **Show raw routing configuration** button lets you 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 fields in the **Routing Configuration** dialog box. If **System IP type** is set to IPv4 + IPv6, the dialog box contains two essentially identical sections, one for each IP type. Each section contains the input fields listed below, a table showing the defined routing rules, and buttons for adding and deleting routes.

Table 4-2   Routing Configuration dialog box

Field	Description
Host/Network	The IP address of the destination network host or segment.
Prefix length	The prefix length that, together with the **Host/Network** address, defines the subnet for this route. For IPv4, a prefix length of 24 is equivalent to specifying a subnet mask of 255.255.255.0. A prefix length of 16 is equivalent to specifying a subnet mask of 255.255.0.0.
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:

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 RealPresence Resource Manager or CMA system or part of a supercluster. The integration must first be terminated or the cluster removed from the supercluster. See "Resource Management System Integration" on page 185 or "Superclustering" on page 227.
>
> 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+07 POSIX).
	If you really want to use a generic GMT offset (for instance, to prevent automatic daylight saving time adjustments), note that they use the Linux/Posix convention of specifying how many hours ahead of or behind local time GMT is. Thus, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.
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:

Licenses

The Polycom DMA system is licensed for the number of concurrent calls it can handle and optionally for API access. See "License the Polycom DMA System" on page 26 for more information about licensing.

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

Table 4-4   Fields on the Licenses page

Field	Description
Active License	
Licensed calls	The maximum number of concurrent calls that the license enables.
Licensed capabilities	Currently, the only separately licensed capability is access to the RealPresence Platform API.
	Note: An API license isn't required in order for a Polycom RealPresence Resource Manager system to access the API. It's only needed for a client application you or a third party develop.

Table 4-4   Fields on the Licenses page (continued)

Field	Description
Activation Keys	
A two-server cluster has two sets of the fields below, one for each server 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:

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

On this page, you can also:

• Turn on H.235 authentication for H.323 devices.

• Turn on SIP digest authentication for SIP devices.

• Click a **Device authentication settings** link to go to the **Device Authentication** page, where you can configure SIP device authentication and maintain the inbound device authentication list for both H.323 and SIP devices (see "Device Authentication" on page 264).

> **Note**
>
> You can turn authentication off and on for specific devices (assuming that it's turned on here for that device type). See "Edit Device Dialog Box" on page 98.

- Configure specific ports or prefixes for "unauthorized" or "guest" SIP calls that can only access specific resources (VMRs, VEQs, or a SIP peer).

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 it's a signaling request (ARQ, BRQ, DRQ) from an unregistered endpoint, the Call Server doesn't authenticate the credentials.
- If it's a signaling request from a registered endpoint, or if the request is from an MCU or neighbor gatekeeper, the Call Server attempts to authenticate using its device authentication list (see "Device Authentication" on page 264).

If the credentials can't be authenticated, the Call Server rejects the registration or signaling request. For call signaling requests, it also rejects the request if the credentials differ from those with which the device registered.

SIP Device Authentication

The SIP digest authentication mechanism is described in RFC 3261, starting in section 22, and in RFC 2617, section 3). When a SIP endpoint registers with or calls the Polycom DMA system, if the request includes authentication information, that information is checked against the Call Server's local device authentication list (see "Device Authentication" on page 264).

SIP authentication can be enabled at the port/transport level or (for "unauthorized" access prefixes) the prefix level. If SIP authentication is enabled and an endpoint's request doesn't include authentication information, the Call Server responds with an authentication challenge containing the required fields (see the RFCs). If the endpoint responds with valid authentication information, the system accepts the registration or call.

> **Note**
>
> If inbound SIP authentication is turned on for a port or prefix, the Polycom DMA system challenges any SIP message coming to the system via that port or with that prefix. Any SIP peer and other device that interacts with the system by those means must be configured to authenticate itself, or you must turn off **Device authentication** for that specific device. See "Edit Device Dialog Box" on page 98.

Untrusted SIP Call Handling Configuration

You can configure special handling for SIP calls from devices outside the corporate firewall that aren't registered with the Polycom DMA system and aren't from a federated division or enterprise. These calls ome to the DMA system via session border controllers (SBCs) such as a Polycom RealPresence Access Director or Acme Packet Session Border Controller device.

For security purposes, you can route such "unauthorized" or "guest" calls to one or more specific VMRs (virtual meeting rooms) or VEQs (virtual entry queues), or to a specific SIP peer. You do so by creating a separate set of "guest" dial rules used only for these untrusted calls. See "Dial Rules" on page 243.

Depending on the SBC and how it's configured, such calls can be distinguished in one of two ways:

- By port: The SBC routes untrusted calls to a specific port.

- By prefix: The SBC adds a specific prefix in the Request-URI of the first INVITE message for the call.

The RealPresence Access Director SBC supports only the prefix method. The Acme Packet Session Border Controller SBC can be configured for either.

In the **SIP Settings** section of the page, you can add one or more ports, prefixes, or both for untrusted calls. For each entry, you can specify whether authentication is required. Calls to an untrusted call prefix follow the authentication setting for that prefix, not for the port on which they're received. For port entries, you can also specify the transport, and if TLS, whether certificate validation is required (mTLS).

> **Note**
>
> If **Skip certificate validation for encrypted signaling** is turned off on the **Security Settings** page, then **Require certificate validation for TLS** is turned on for both authorized and unauthorized ports, and it can't be turned off. See "Security Settings" on page 48.

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 the 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 for more information.

Signaling Settings Fields

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

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

Field	Description
H.323 Settings	
Enable H.323 signaling	Enables the system to receive H.323 calls. **Caution:** Disabling H.323 terminates any existing H.323 calls. When you click **Update**, the system prompts you to confirm.
Status	Indicates whether the system's H.323 gatekeeper functions are active.
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 RAS (Registration, Admission and Status). 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.
Enable H.323 device authentication	Check the box to turn on H.323 device authentication. Click **Device authentication settings** to go to the **Device Authentication** page and add authentication credentials (see "Device Authentication" on page 264).
SIP Settings	
Enable SIP signaling	Enables the system to receive Session Initiation Protocol (SIP) calls. **Caution:** Disabling SIP terminates any existing SIP calls. When you click **Update**, the system prompts you to confirm.

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

Field	Description
Authorized ports	
Unencrypted SIP port	To permit unencrypted SIP connections, select either **TCP** or **UDP/TCP** from the list. Select **None** to disallow unencrypted SIP connections. 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 and from any "unauthorized" or "guest" ports that your SBC(s) may be configured to use for calls to the system.
Enable authentication	Check the box to turn on SIP device authentication for unencrypted SIP. Click the **Device authentication settings** link to go to the **Device Authentication** page to configure SIP device authentication and add device authentication credentials (see "Device Authentication" on page 264). The settings on that page determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required).
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 and from any "unauthorized" or "guest" ports that your SBC(s) may be configured to use for calls to the system. If SIP signaling is enabled, TLS is automatically supported. Unless unencrypted SIP connections are specifically permitted, TLS must be used.
Enable authentication	Check the box to turn on SIP device authentication for encrypted SIP. Click the **Device authentication settings** link to go to the **Device Authentication** page to configure SIP device authentication and add device authentication credentials (see "Device Authentication" on page 264). The settings on that page determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required).
Require certificate validation for TLS	Check the box to enable mutual TLS (mTLS), requiring each caller to present a valid certificate.

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

Field	Description
Unauthorized ports	Lists the ports used by your SBC(s) for untrusted calls, showing the transport type for each and, for TLS, whether a certificate is required. The **Authentication** column indicates whether calls to that port are passed without challenge, challenged for authentication credentials, or blocked.
	Click **Add** to add a port to the list (see "Add Guest Port Dialog Box" on page 77). Click **Edit** to edit the selected entry (see "Edit Guest Port Dialog Box" on page 78) or **Delete** to delete it.
Unauthorized prefixes	Lists the prefixes used by your SBC(s) for untrusted calls. The **Strip Prefix** column indicates whether the DMA system should immediately strip the prefix. The **Authentication** column indicates whether calls to that port are passed without challenge, challenged for authentication credentials, or blocked.
	Click **Add** to add a prefix to the list (see "Add Guest Prefix Dialog Box" on page 79). Click **Edit** to edit the selected entry (see "Edit Guest Prefix Dialog Box" on page 80) or **Delete** to delete it.
XMPP Settings	
Enable XMPP signaling	Enables the system to act as an Extensible Messaging and Presence Protocol (XMPP) server for chat and presence services.
	Caution: Disabling XMPP terminates any existing XMPP logins. When you click **Update**, the system prompts you to confirm.
Unencrypted XMPP port	If security settings permit unencrypted XMPP connections (see "Security Settings" on page 48), 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 "Security Settings" on page 48.

See also:

Add Guest Port Dialog Box

The **Add Guest Port** dialog box appears when you click the **Add** button next to the **Unauthorized ports** list in the **SIP Settings** section of the **Signaling Settings** page. It lets you add a port to the list of ports used for "unauthorized" or "guest" calls.

The following table describes the fields in the **Add Guest Port** dialog box.

Table 4-6   *Add Guest Port dialog box*

Field	Description
Port	The SIP signaling port number for this entry. This is the port number that an SBC is configured to use for untrusted calls to the DMA system via the transport specified below.
Transport	The transport supported on this port.
Require certificate validation for TLS	For TLS transport, check this box to enable mutual TLS (mTLS), requiring callers to present a valid certificate. **Note:** If **Skip certificate validation for encrypted signaling** is turned off on the **Security Settings** page, then **Require certificate validation for TLS** is turned on for both authorized and unauthorized ports, and it can't be turned off. See "Security Settings" on page 48.
Authentication	Select one of the following: • **None** — The system doesn't issue authentication challenges or check authentication credentials for calls to this port. • **Authenticate** — The system issues authentication challenges and checks authentication credentials for calls to this port. The settings on the **Device Authentication** page (see "Device Authentication" on page 264) determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required). • **Block** — The system blocks calls to this port.

See also:

Edit Guest Port Dialog Box

The **Edit Guest Port** dialog box lets you edit an **Unauthorized ports** list entry in the **SIP Settings** section of the **Signaling Settings** page.

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

Table 4-7   Edit Guest Port dialog box

Field	Description
Port	The SIP signaling port number for this entry.
	This is the port number that an SBC is configured to use for untrusted calls to the DMA system via the transport specified below.
Transport	The transport supported on this port.
Require certificate validation for TLS	For TLS transport, check this box to enable mutual TLS (mTLS), requiring callers to present a valid certificate.
	Note: If **Skip certificate validation for encrypted signaling** is turned off on the **Security Settings** page, then **Require certificate validation for TLS** is turned on for both authorized and unauthorized ports, and it can't be turned off. See "Security Settings" on page 48.
Authentication	Select one of the following:
	• **None** — The system doesn't issue authentication challenges or check authentication credentials for calls to this port.
	• **Authenticate** — The system issues authentication challenges and checks authentication credentials for calls to this port.
	The settings on the **Device Authentication** page (see "Device Authentication" on page 264) determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required).
	• **Block** — The system blocks calls to this port.

See also:

Add Guest Prefix Dialog Box

The **Add Guest Prefix** dialog box appears when you click the **Add** button next to the **Unauthorized prefixes** list in the **SIP Settings** section of the **Signaling Settings** page. It lets you add a prefix to the list of prefixes used for "unauthorized" or "guest" calls.

The following table describes the fields in the **Add Guest Prefix** dialog box.

Table 4-8   *Add Guest Prefix dialog box*

Field	Description
Prefix	The prefix number for this entry. This is the number that an SBC is configured to add to the Request-URI of the first INVITE message for untrusted calls to the DMA system.
Strip prefix	Check this box to have the system immediately strip this prefix from the INVITE message.
Authentication	Select one of the following: • **None** — The system doesn't issue authentication challenges or check authentication credentials for calls with this prefix. • **Authenticate** — The system issues authentication challenges and checks authentication credentials for calls with this prefix. The settings on the **Device Authentication** page (see "Device Authentication" on page 264) determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required). • **Block** — The system blocks calls with this prefix.

See also:

Edit Guest Prefix Dialog Box

The **Edit Guest Prefix** dialog box lets you edit an **Unauthorized prefixes** list entry in the **SIP Settings** section of the **Signaling Settings** page.

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

Table 4-9   *Edit Guest Prefix dialog box*

Field	Description
Prefix	The prefix number for this entry. This is the number that an SBC is configured to add to the Request-URI of the first INVITE message for untrusted calls to the DMA system.
Strip prefix	Check this box to have the system immediately strip this prefix from the INVITE message.
Authentication	Select one of the following: • **None** — The system doesn't issue authentication challenges or check authentication credentials for calls with this prefix. • **Authenticate** — The system issues authentication challenges and checks authentication credentials for calls with this prefix. The settings on the **Device Authentication** page (see "Device Authentication" on page 264) determine the realm used for authentication and whether the Call Server responds to unauthenticated requests with 401 (Unauthorized) or 407 (Proxy Authentication Required). • **Block** — The system blocks calls with this prefix.

See also:

Logging Settings

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

Table 4-10   *Fields on the Logging Settings page*

Field	Description
Logging level	Leave the default, **Production**, unless advised to change it by Polycom support. **Debug** is useful for troubleshooting. **Verbose debug** 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. For most systems, we recommend setting this to 7.
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	Enables you to forward selected log entries to a central log management server (such as Graylog2). Specify: • The address of the destination server. It must be running some version of syslog. • 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. • The facility value. Default is **Local0**. • The log or logs to forward. **Note:** 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 are assigned the syslog-compliant "notice" severity. 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.

See also:

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 23 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 70

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.

d To turn on H.235 authentication, select **Enable H.323 device authentication**.

Device authentication credentials must be added on the **Inbound Authentication** tab of the **Device Authentication** page. Click the **Device authentication settings** link to go directly there.

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 set **Unencrypted SIP port** to **TCP** or **UDP/TCP**.

You must have the Administrator role to change security settings. See "Security Settings" on page 48.

Note

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

For more information about this and other aspects of SIP, see RFC 3261.

---

c Leave the default port numbers (5060 for TCP/UDP, 5061 for TLS) unless you have a good reason for changing them.

d To turn on SIP digest authentication for either the unencrypted or TLS port, select the corresponding **Enable authentication** check box.

Device authentication credentials must be added on the **Inbound Authentication** tab of the **Device Authentication** page. Click the **Device authentication settings** link to go directly there.

e To enable mutual TLS (mTLS), select **Require certificate validation for TLS**.

4 To enable the system to receive untrusted calls (see "Untrusted SIP Call Handling Configuration" on page 73) from SIP session border controllers (SBCs) configured to route such calls to special ports, do the following:

a Under **Unauthorized ports**, click **Add**.

The **Add Guest Port** dialog box opens.

b Specify the port number, the transport, whether authentication is required, and for TLS, whether certificate validation is required (mTLS). Click **OK**.

The new entry is added to the **Unauthorized ports** list.

c Repeat for each additional port on which to receive "unauthorized" or "guest" calls.

5 To enable the system to receive untrusted calls (see "Untrusted SIP Call Handling Configuration" on page 73) from SIP session border controllers (SBCs) configured to add a specific prefix in the Request-URI of the INVITE message for such calls, do the following:

a Under **Unauthorized prefixes**, click **Add**.

The **Add Guest Prefix** dialog box opens.

b Specify the prefix number, whether it should be stripped, and whether authentication is required. Click **OK**.

The new entry is added to the **Unauthorized prefixes** list.

c Repeat for each additional prefix used for "unauthorized" or "guest" calls.

6 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 48.

c Leave the default port numbers (5222 for unencrypted XMPP, 5223 for TLS) unless you have a good reason for changing them.

7 Click **Update**.

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

8 Click **OK**.

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

9 If you enabled the system to receive "unauthorized" or "guest" calls, do the following:

a Go to **Admin > Call Server > Dial Rules** and click in the **Dial rules for unauthorized calls** list to give it focus.

b Add one or more dial rules to be used for routing "unauthorized" or "guest" calls. See "Dial Rules" on page 243.

An unauthorized call rule can route calls to a conference room ID (virtual meeting room, or VMR), a virtual entry queue (VEQ), or a SIP peer.

See also:

"Signaling Settings" on page 71

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 81

5

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:

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.

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 89 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, when available.
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:

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
Call Info	
Call Info	Displays the call's: • Status (active/ended and pinned/unpinned) • Start time and end time • Duration • Signaling protocol(s) • Polycom DMA server(s) involved • Unique call ID • Dial string, if available • Final dial string (after processing by dial rules)
Originator	Displays the source device's: • Name and authentication name • Authentication status • Model and version • Aliases • IP address or host name • Registration status • Site and territory If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.
Destination	Displays the destination device's: • Name and authentication name • Authentication status • Model and version • Aliases • IP address or host name • Registration status • Site and territory If this is a registered endpoint or a registered/configured MCU, a link takes you to the corresponding page with that endpoint or MCU selected.

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

Tab/Field/Column	Description
Bandwidth	The table at the top lists each throttle point that the call traverses and shows its: • Bit rate limit per call (kbps) • Total capacity (kbps) • Used bit rate (kbps) in each class of service • Weight (%) • Territory If the throttle point is a subnet, site, or site link, a link takes you to the corresponding site topology page with the throttle point entity selected. Below the table, the data used in bandwidth processing is displayed (all bit rates are kbps): • Formal maximum bit rate limit — the maximum allowed bit rate considering the per call bit rates of each throttle point, but not considering total capacity or current usage • Available bit rate capacity in each class of service and for the call's class • Class of service for the call • Minimum downspeed bit rate • Available bit rate limit (%) — the maximum percentage of remaining bandwidth at a throttle point that will be given to any one call (configurable on the Call Server Settings page) • Requested bit rate • Final bit rate
Call Events	Lists each event in the call and its attributes. When the system is operating as a SIP proxy server, the list includes all SIP signaling messages except 100 TRYING. Hover over an attribute label to see a description. Click **Show Message** to see the signaling message. Click **Show QoS Data** to see detailed quality of service statistics.
Property Changes	Lists each property change in the call, showing the value, time, and sequence number of the associated event.
QoS	Quality of service data is only available if one of the endpoints is a registered H.323 endpoint that supports IRQs. This tab displays a graph showing how QoS varied during the call. The horizontal scale and frequency of data points (dots on the lines of the graph) vary based on the length of the call. Hover over a data point to see the value at that point.

See also:

"Active Calls" on page 87

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 268), inactive devices may be automatically deleted after a specified number of days.

*   Select multiple devices to block/unblock, quarantine/unquarantine, delete, or change specific settings of (device authentication, permanent registration, and class of service).

*   Manually add a device. The registration status of the device depends on the system's registration policy (see "Add Device Dialog Box" on page 96).

*   Associate a user with a device.

> **Note**
>
> If the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom RealPresence Resource Manager or 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: • Gold • Silver • Bronze • Inherit from associated user (if none, default to Bronze)
Admission Policy	Indicates the admission policy applied to the device: • Allow • Block • Quarantine • Reject
Compliance Level	Indicates whether the device is compliant or noncompliant with the applicable registration policy script (see "Registration Policy" on page 268).

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

Column	Description

Status	The registration status of the device:
	• Active — The device is registered and can make and receive calls.
	• Inactive — The device's registration has expired. Whether it can make and receive calls depends on the system's rogue call policy (see "Call Server Settings" on page 239) and. It can register again.
	• 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.
	• Quarantined (Inactive) — The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status.
	• Blocked — The device is not permitted to register. It remains blocked from registering until you unblock it.
	  If the device is in a site managed by the system, its ability to make and receive calls depends on the system's rogue call policy (see "Call Server Settings" on page 239).
	  If the device is not in a site managed by the system, it can't make or receive calls.
	A device's status can be determined by:
	• An action by the device.
	• An action applied to it manually on this page.
	• The expiration of a timer.
	• The application of a registration policy and admission policy (see "Registration Policy" on page 268).

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.
Device Authentication	Indicates whether the endpoint must authenticate itself. **Note:** Inbound authentication for the device type must be enabled at the system level (see "Device Authentication" on page 264), or the setting for the device has no effect.

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 **Device Details** dialog box for the selected endpoint.
Add	Opens the **Add Device** dialog box, where you can manually add a device to the system.
Edit	Opens the **Edit Device** dialog box for the selected endpoint, where you can change its information and settings. If multiple endpoints are selected, opens the **Edit Devices** dialog box, where you can change the device authentication, permanent registration, and class of service settings.
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 "Call Server Settings" on page 239). 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 **Unblock**.
	If a blocked device is in a site managed by the system, its ability to make and receive calls depends on the system's rogue call policy (see "Call Server Settings" on page 239). If the device is not in a site managed by the system, it can't make or receive calls.
Quarantine	Prevents the endpoint(s) from making or receiving calls. A dialog box asks you to confirm. When quarantined endpoints are selected, this becomes **Unquarantine**.
	Unlike a blocked endpoint, a quarantined endpoint is registered (or can register) with the Call Server.
Associate User	Opens the **Associate User** 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 RealPresence Resource Manager or CMA system. In that case, it receives user-to-device association information from that system.
View Call History	Takes you to **Reports > Call History** and displays the call history for the selected endpoint.
View Registration History	Takes you to **Reports > Registration History** 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 239).

*   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_3_1
> Bainbridge ITP_3_2
> Bainbridge ITP_3_3

The Polycom DMA system would recognize these three registrations as constituting a single ITP system and assign them a Gold class of service (you can change this if you wish).

The Polycom DMA system also manages the device authentication settings as applying to a single system. You can only edit the device authentication and class of service 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.

> **Note**
>
> The Polycom DMA system's ability to recognize ITP calls and treat them as one assures the same class of service and device authentication settings for all the endpoints in the ITP system, but not other registration settings. It's up to you to ensure that the maximum and minimum bit rates and other registration settings are consistent.
>
> This capability also doesn't ensure the availability of sufficient MCU ports for all the endpoints (codecs) in the ITP system. For multi-point conferencing, we recommend dedicating an MCU pool for your ITP system(s).

This capability is only available for H.323.

Follow this naming convention for both the HDX system name and the H.323 name for each HDX endpoint in the ITP system. For more information, see the following documents:

• *Administrator's Guide for Polycom HDX Systems*

• *Polycom Immersive Telepresence (ITP) Deployment Guide*

• *Polycom Multipoint Layout Application (MLA) User's Guide for Use with Polycom Telepresence Solutions*

See also:

"Device Management" on page 87

"Add Device Dialog Box" on page 96

"Edit Device Dialog Box" on page 98

"Associate User Dialog Box" on page 101

"Active Calls" on page 87

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 268) 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	For an H.323 device, the H.225 call signaling address (and optionally, port) of the device. Either this or the RAS address is required.
RAS address	For an H.323 device, the RAS (Registration, Admission and Status) channel address (and optionally, port) of the device.
Aliases	For an H.323 device, lists the device's aliases. When you're adding a device, this list is empty. The **Add** button lets you add an alias.
Address of record	For a SIP device, the AOR with which the device registers (see registration rules in RFC 3261), such as: sip:1000@westminster.polycom.com
Device authentication	Indicates whether the endpoint must authenticate itself. **Note:** Inbound authentication for the device type must be enabled at the system level (see "Device Authentication" on page 264), or the setting for the device has no effect.
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:

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
Device type	The device's signaling protocol (H.323 or SIP).
Signaling address	For an H.323 device, the H.225 call signaling address (and optionally, port) of the device. Either this or the RAS address is required.
RAS address	For an H.323 device, the RAS (Registration, Admission and Status) channel address (and optionally, port) of the device.
Aliases	For an H.323 device, lists the device's aliases. When you're adding a device, this list is empty. The **Add** button lets you add an alias.
Site	The site to which the device belongs. Display only.
Owner domain	The domain to which the device's owner belongs, if provided by the device. Display only.
Owner	The user who owns the device, if provided by the device. Display only.
Registration status	The registration status of the device. Display only.
Permanent	Prevents the registration from ever expiring.
Device authentication	Indicates whether the endpoint must authenticate itself. **Note:** Inbound authentication for the device type must be enabled at the system level (see "Device Authentication" on page 264), or the setting for the device has no effect.
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.

Table 5-6   *Edit Device dialog box (continued)*

Field	Description
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 91

"Add Alias Dialog Box" on page 100

"Edit Alias Dialog Box" on page 100

Edit Devices Dialog Box

The **Edit Devices** dialog box appears when you select multiple devices on the **Endpoints** page and click **Edit Devices**. It lets you change certain settings for multiple devices at a time.

The following table describes the parts of the dialog box.

Table 5-7   *Edit Device dialog box*

Field	Description
Device authentication	Indicates whether the selected devices must authenticate themselves. **Note:** Inbound authentication for the device type must be enabled at the system level (see "Device Authentication" on page 264), or the setting for these devices has no effect.
Permanent	Prevents the registration of the selected devices from ever expiring.

Table 5-7   *Edit Device dialog box (continued)*

Field	Description
Class of service	Select to modify the class of service and the bit rate limits for calls to and from the selected devices. A call between two devices receives the higher class of service of the two.
Maximum bit rate (kbps)	The maximum bit rate for calls to and from the selected devices.
Minimum downspeed bit rate (kbps)	The minimum bit rate to which calls from the selected devices can be downspeeded to manage bandwidth. If this minimum isn't available, the call is dropped.

See also:

Add Alias Dialog Box

The **Add Alias** dialog box lets you specify an alias for the H.323 device you're adding or editing. Enter the alias in the **Value** box and click **OK**.

See also:

Edit Alias Dialog Box

The **Edit Alias** dialog box lets you change the selected alias for the H.323 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:

Associate User Dialog Box

> **Note**
>
> If the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom RealPresence Resource Manager or 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:

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 5-8   *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. **Note:** 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.

Table 5-8   *Information in the Site Statistics list (continued)*

Column	Description
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:

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 5-9   *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. **Note:** 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.

Table 5-9   *Information in the Site Link Statistics list (continued)*

Column	Description
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:

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 250) 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 5-10   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 *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution.
Enabled	Indicates whether the system is using the neighbor gatekeeper.

See also:

Add External Gatekeeper Dialog Box

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

Table 5-11   Add External Gatekeeper dialog box

Column	Description
External Gatekeeper	
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 **External Gatekeepers** 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.

Table 5-11   *Add External Gatekeeper dialog box*

Column	Description
Prefix range	The dial string prefix or prefix range for which the external gatekeeper is responsible. Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49). If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution. If your dial plan instead uses a rule that you create to apply the **Resolve to external gatekeeper** action, there is no need to specify a prefix.
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this gatekeeper.
Prefer routed	If selected (the default), the system forces a call to this gatekeeper to routed mode if: • The gatekeeper is configured with a prefix. • The destination signaling address in the gatekeeper's location confirm (LCF) message contains its own IP address (indicating that it's in routed mode). This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.
Authentication Mode	In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.
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.

Table 5-11   *Add External Gatekeeper 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 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 **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

"External Gatekeeper" on page 103

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

"Device Authentication" on page 264

Edit External Gatekeeper Dialog Box

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

Table 5-12   *Edit External Gatekeeper dialog box*

Column	Description
External Gatekeeper	
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 **External Gatekeepers** 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.

Table 5-12   *Edit External Gatekeeper dialog box*

Column	Description
Prefix range	The dial string prefix or prefix range for which the external gatekeeper is responsible.
	Enter a single prefix (44), a range of prefixes (44-47), multiple prefixes separated by commas (44,46), or a combination (41, 44-47, 49).
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this gatekeeper for resolution.
	If your dial plan instead uses a rule that you create to apply the **Resolve to external gatekeeper** action, there is no need to specify a prefix.
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this gatekeeper.
Prefer routed	If selected (the default), the system forces a call to this gatekeeper to routed mode if:
	• The gatekeeper is configured with a prefix.
	• The destination signaling address in the gatekeeper's location confirm (LCF) message contains its own IP address (indicating it's in routed mode).
	This setting must be enabled to avoid interoperability issues with Polycom CMA and Avaya gatekeepers, and possibly others as well.
Authentication Mode	In this section, you can configure the system to send its H.235 credentials when it sends address resolution requests to that gatekeeper.
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.

Table 5-12   Edit External Gatekeeper 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 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 **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

"External Gatekeeper" on page 103

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

"Device Authentication" on page 264

External SIP Peer

On the **External SIP Peer** page, you can add or remove SIP servers or devices from the list of SIP peers 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 the need for external SIP peer servers (other than SIP session border controllers, or SBCs).

The following table describes the fields in the list.

Table 5-13   Fields in the External SIP Peer list

Column	Description
Name	The name of the SIP peer.
Description	Brief description of the SIP peer.
Next Hop Address	Fully qualified domain name (FQDN) or IP address of the SIP peer

Table 5-13   Fields in the External SIP Peer list (continued)

Column	Description
Prefix Range	The dial string prefix(es) assigned to this SIP peer.
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.
Enabled	Indicates whether the system is using the SIP peer.
Outbound	Indicates whether the system is registered with the SIP peer so that it can route calls to it.

See also:

Add External SIP Peer Dialog Box

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

Table 5-14   Add External SIP Peer dialog box

Field	Description
External SIP Peer	
Enabled	Clearing this check box lets you stop using an external SIP peer without deleting it.
Name	Peer name or number. Must be unique among SIP peers.
Description	The text description displayed in the **External SIP Peer** list.
Next hop address	Fully qualified domain name (FQDN), host name, or IP address of the SIP peer.
	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).

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

Field	Description
Destination network	Host name, FQDN, or network domain label of the SIP peer, with or without port and URL parameters.
	If specified, this value by default replaces the non-user portion of a URL (after the @ symbol) of the To header and Request-URI for forwarded messages, and just the Request-URI for REGISTER messages.
	If **Type** is set to Microsoft, this field is required, is used for the peer's domain, and is implicitly added to the **Domain List** (if not already there).
Port	The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, specify it.
	If left blank, the system uses the full RFC 3263 procedure to determine the port via DNS.
Use route header	Add a Route header with the peer's **Next hop address** value to the message. Applies to both forwarded messages and external REGISTER messages.
	If not selected, the only valid Request-URI configurations are those that use the peer's **Next hop address** value for the URI host.
Prefix range	The dial string prefix(es) assigned to this SIP peer.
	Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SIP peer for resolution.
	Note: For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to alice@polycom.com must be one of the following: sip:123alice@polycom.com sips:123alice@polycom.com 123alice
	If your dial plan instead uses a rule that you create to apply the *Resolve to external SIP peer* action, there is no need to specify a prefix.
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.

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

Field	Description
Type	For a Microsoft Office Communications Server or Lync Server 2010, select **Microsoft**. Otherwise, select **Other**. Selecting **Microsoft** implicitly adds the **Destination network** value to the **Domain List** (if not already there) and automatically selects the **Postliminary** settings that are correct for most deployments with Lync Server 2010, but you can modify them if necessary.
Transport type	The transport protocol to use when contacting this SIP peer. The default is **UDP**. **Auto detect** tells the system to select the protocol using DNS as specified in RFC 3263, and is not valid if **Next hop address** is a numeric IP address instead of a host/domain name.
Downgrade	If selected, and if this peer doesn't support TLS, the system can change the Request-URI schema from sips to sip and route the call to this peer. If not selected, the system routes a TLS call to this peer only if this peer supports TLS.
Register externally	Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also referred to as *pilot registration*). Select this option to enable the **External Registration** tab and configure the system to register with this external SIP peer, following the rules specified in RFC 3261.
Domain List	If your dial plan uses a rule to apply the *Resolve to external SIP peer* action, you can restrict calls to this SIP peer to specific domains by adding the authorized domains to this list. If this list is empty, all domains can resolve to this peer. **Note:** In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict SIP peers to specific domains.
Add new domain	Enter a domain and click **Add** to add it to the list of authorized domains.
Authorized domains	List of administrative domains, contained in the dial string, for which calls are routed to this SIP peer. Leave this list empty to route any call that matches the rule to this SIP peer. Select a domain and click **Remove** to remove it from the list.

Table 5-14   Add External SIP Peer dialog box

Field	Description
Postliminary	
Use output format	Enables dial string transformations using the To header and Request-URI option settings below instead of a customized script.
	Note: The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select **Use customized script**.
	To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes.
To header options	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 **Free Form Template** and define the format in the associated **Template** field.
	The predefined formats in the list and the variables you use in the **Template** field are described in "SIP Peer Postliminary Output Format Options" on page 119.
Request URI options	Specify the format of the Request-URI.
Format Template	Select a predefined format from the list, or select **Free Form Template** and define the format in the associated **Template** field.
	The predefined formats in the list and the variables you use in the **Template** field are described in "SIP Peer Postliminary Output Format Options" on page 119.
Use customized script	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.
	Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.
	Note: When you make settings in the **Use output format** section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script.

Table 5-14   Add External SIP Peer dialog box

Field	Description
Authentication	On this tab, you can configure SIP digest authentication, as specified in RFC 3261, for this SIP peer and add or edit authentication credentials. SIP authentication must be enabled and configured on the Device Authentication page. **Note:** The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the *Resolve to external SIP peer* action. If another dial rule action, such as *Resolve to external address*, is applied to the call, there is no association to this peer and its authentication settings aren't used.
Authentication	Select one: • Handle authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials. • Pass authentication — When it receives a 401 response from this SIP peer, the Call Server passes it to the source of the request. **Note:** SIP authentication requests are never passed to an H.323 endpoint (a gateway call). If the Call Server can't provide the required credentials, the call fails.
Proxy authentication	Select one: • Handle proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials. • Pass proxy authentication — When it receives a 407 response from this SIP peer, the Call Server passes it to the source of the request. **Note:** Authentication requests are never passed to an H.323 endpoint (a gateway call). If the Call Server can't provide the required credentials, the call fails.
(table of authentication entries)	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 **Add** to add authentication credentials. 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 Device Authentication page.
External Registration	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.

See also:

Edit External SIP Peer Dialog Box

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

Table 5-15   *Edit External SIP Peer dialog box*

Field	Description
External SIP Peer	
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 **External SIP Peer** 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, FQDN, or network domain label 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 **Type** is set to Microsoft, this field is required, is used for the peer's domain, and is implicitly added to the **Domain List** (if not already there).

Table 5-15   *Edit External SIP Peer dialog box*

Field	Description
Port	The SIP signaling port number. Defaults to the standard UDP/TCP port, 5060. If the peer server is using a different port number, specify it.
	If left blank, the system uses the full RFC 3263 procedure to determine the port via DNS.
Use route header	Add a Route header with the peer's **Next hop address** value to the message. Applies to both forwarded messages and external REGISTER messages.
	If not selected, the only valid Request-URI configurations are those that use the peer's **Next hop address** value for the URI host.
Prefix range	The dial string prefix(es) assigned to this peer server.
	Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this peer server for resolution.
	Note: For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to alice@polycom.com must be one of the following:
	sip:123alice@polycom.com
	sips:123alice@polycom.com
	123alice
	If your dial plan instead uses a rule that you create to apply the *Resolve to external SIP peer* action, there is no need to specify a prefix.
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this peer.
Type	For a Microsoft Office Communications Server or Lync Server 2010, select **Microsoft**. Otherwise, select **Other**.
	Selecting **Microsoft** implicitly adds the **Destination network** value to the **Domain List** (if not already there) and automatically selects the **Postliminary** settings that are correct for most deployments with Lync Server 2010, but you can modify them if necessary.
Transport type	The transport protocol to use when contacting this peer server. The default is **UDP**.
	Auto detect tells the system to select the protocol as specified in RFC 3263, and is not valid if **Next hop address** is a numeric IP address instead of a host/domain name.

Table 5-15   *Edit External SIP Peer dialog box*

Field	Description
Downgrade	If selected, and if this peer doesn't support TLS, the system can change the Request-URI schema from sips to sip and route the call to this peer.
	If not selected, the system routes a TLS call to this peer only if this peer supports TLS.
Register externally	Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message.
	Select this option to enable the **External Registration** tab and configure the system to register with this external peer server, following the rules specified in RFC 3261.
Domain List	If your dial plan uses a rule to apply the *Resolve to external SIP peer* action, you can restrict calls to this peer server to specific domains by adding the authorized domains to this list.
	If this list is empty, all domains can resolve to this peer.
	Note: In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict peer servers to specific domains.
Add new domain	Enter a domain and click **Add** to add it to the list of authorized domains.
Authorized domains	List of administrative domains, contained in the dial string, for which calls are routed to this peer server.
	Leave this list empty to route any call that matches the rule to this peer server.
	Select a domain and click **Remove** to remove it from the list.
Postliminary	
Use output format	Enables dial string transformations using the To header and Request-URI option settings below instead of a customized script.
	Note: The system generates a script that implements the settings made in this section. To see (and perhaps copy) the generated script, you can temporarily select **Use customized script**.
	To help you learn how to write your own script, you can make different settings in this section and see how the generated script changes.
To header options	Specify the format of the To header in messages sent to this peer.

Table 5-15 Edit External SIP Peer dialog box

Field	Description
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 **Free Form Template** and define the format in the associated **Template** field. The predefined formats in the list and the variables you use in the **Template** field are described in "SIP Peer Postliminary Output Format Options" on page 119.
Request URI options	Specify the format of the Request-URI.
Format Template	Select a predefined format from the list, or select **Free Form Template** and define the format in the associated **Template** field. The predefined formats in the list and the variables you use in the **Template** field are described in "SIP Peer Postliminary Output Format Options" on page 119.
Use customized script	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. Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables. **Note:** When you make settings in the **Use output format** section, the system generates a script that implements those settings. Select this option to see (and perhaps copy) the generated script.
Authentication	On this tab, you can configure SIP digest authentication, as specified in RFC 3261, for this SIP peer and add or edit authentication credentials. SIP authentication must be enabled and configured on the Device Authentication page. **Note:** The digest authentication settings for this peer are used only in conjunction with a dial rule specifying the *Resolve to external SIP peer* action. If another dial rule action, such as *Resolve to external address*, is applied to the call, there is no association to this peer and its authentication settings aren't used.

Table 5-15   Edit External SIP Peer dialog box

Field	Description
Authentication	Select one: • Handle authentication — When it receives a 401 (Unauthorized) response from this SIP peer, the Call Server presents its authentication credentials. • Pass authentication — When it receives a 401 response from this SIP peer, the Call Server passes it to the source of the request. **Note:** SIP authentication requests are never passed to an H.323 endpoint (a gateway call). If the Call Server can't provide the required credentials, the call fails.
Proxy authentication	Select one: • Handle proxy authentication — When it receives a 407 (Proxy Authentication Required) response from this SIP peer, the Call Server presents its authentication credentials. • Pass proxy authentication — When it receives a 407 response from this SIP peer, the Call Server passes it to the source of the request.
(table of authentication entries)	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 **Add** to add authentication credentials. 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 Device Authentication page.
External Registration	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.

See also:

"External SIP Peer" on page 108

"SIP Peer Postliminary Output Format Options" on page 119

"Device Authentication" on page 264

"Add Authentication Dialog Box" on page 123

"Edit Authentication Dialog Box" on page 123

"Add Outbound Registration Dialog Box" on page 124

"Edit Outbound Registration Dialog Box" on page 125

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

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 Header Format Options

- Free Form Template Variables

- To Header and Request-URI Header 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 121 and "To Header and Request-URI Header Examples" on page 122.

Request-URI Header Format Options

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

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

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

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

`#orscheme#:#orhost#`

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

`#pscheme#:#phost#`

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

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

Note

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

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

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

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

`#pscheme#:#pnetORphost#`

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

`#pscheme#:#otuser#@#pnetORphost#`

Default Request-URI for Microsoft. — Equivalent to template:

`sip:#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 121 and "To Header and Request-URI Header Examples" on page 122.

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 124), 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 5-16   *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 (next hop address).
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.
pport	The port specified for this SIP peer.
ptransport	The transport type specified for this SIP peer.

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

For the Request-URI, the contents of the Template field specify only the URI portion of the full Request line. Depending on network configuration, a Route header may be required.

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

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

To Header and Request-URI Header Examples

The tables below show some examples of To header and Request-URI header transformations using the variables described in "Free Form Template Variables" on page 121.

Table 5-17   *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:foo.bar`
`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@toHeaderUrlHost`

Table 5-18   *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:

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 114) or to the general list of outbound authentication credentials that the system uses if challenged by an external device (see "Device Authentication" on page 264).

The following table describes the fields in the dialog box.

Table 5-19   *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:

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 114) or from the general list of outbound credentials for the system (see "Device Authentication" on page 264).

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

Table 5-20   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:

Add Outbound Registration Dialog Box

Some external SIP peers require peers to register with them as an endpoint does, using a REGISTER message (also known as *pilot registration*). 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 5-21   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.

Table 5-21   Add Outbound Registration dialog box

Field	Description
Contact address format	Select **IP** or **DNS** to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it re-sends the registration using its IP address or DNS name. Select **Free Form** to specify that the contact header should use the FQDN you enter. The external 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. **Note:** The authentication credentials specified here are specific to this SIP peer and are not tied to any other authentication configuration values.
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 121.
Other headers	Additional headers to include when registering with this SIP peer. Click **Add** to add a header. In the **Add Header** dialog box, specify the header name and value(s), using the variables (#delimited) defined in "Free Form Template Variables" on page 121. Click **Edit** or **Delete** to edit or delete the selected header.

See also:

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 5-22   *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.
Contact address format	Select **IP** or **DNS** to specify that the contact header should use the virtual IP address or virtual DNS name of the cluster currently managing the territory. If the territory responsibility switches to the other cluster, it re-sends the registration using its IP address or DNS name. Select **Free Form** to specify that the contact header should use the FQDN you enter. The external 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. **Note:** The authentication credentials specified here are specific to this SIP peer and are not tied to any other authentication configuration values.
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 121.
Other headers	Additional headers to include when registering with this SIP peer. Click **Add** to add a header. In the **Add Header** dialog box, specify the header name and value(s), using the variables (#delimited) defined in "Free Form Template Variables" on page 121. Click **Edit** or **Delete** to edit or delete the selected header.

See also:

External SBC

On the **External SBC** page, you can add or remove H.323 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, H.323 SBCs regulate access across the firewall.

This is a supercluster-wide configuration.

> **Note**
>
> This page is only for H.323 SBCs. SIP SBCs are configured as SIP peers. See "External SIP Peer" on page 108.

For most configurations, H.323 SBCs should be configured on a per site basis on the Sites page. There are three reasons to configure an H.323 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 5-23   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.

Table 5-23   Fields in the External SBC list (continued)

Column	Description
Prefix Range	The dial string prefix(es) assigned to this SBC. If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.
Enabled	Indicates whether the system is using the SBC.

See also:

Add External SBC Dialog Box

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

Table 5-24   Add External SBC dialog box

Column	Description
External SBC	
Enabled	Clearing this check box lets you stop using an external SBC without deleting it.
Name	SBC unit name.
Description	The text description displayed in the **External SBC** 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.

Table 5-24   Add External SBC dialog box

Column	Description
Prefix range	The dial string prefix or prefix range for which the external SBC is responsible.
	Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.
	If you don't specify prefixes, the dial plan can use the *Dial external networks by H.323 URL or SIP URI* dial rule or the *Dial endpoints by IP address* 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 **Add Site** or **Edit Site** dialog (see "Edit Site Dialog Box" on page 292).
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this SBC.
Postliminary	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the SBC.
Enabled	Lets you turn a postliminary on or off without deleting it.
Script	Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

"External SBC" on page 127

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

Edit External SBC Dialog Box

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

Table 5-25   Edit External SBC dialog box

Column	Description
External SBC	
Enabled	Clearing this check box lets you stop using an external SBC without deleting it.
Name	SBC unit name.
Description	The text description displayed in the **External SBC** 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	The dial string prefix or prefix range for which the external SBC is responsible.
	Enter a single prefix (44), a range of prefixes (44-47), or multiple prefixes separated by commas (44,46)
	If your dial plan uses the *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this SBC for resolution.
	If you don't specify prefixes, the dial plan can use the *Dial external networks by H.323 URL or SIP URI* dial rule or the *Dial endpoints by IP address* 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 **Add Site** or **Edit Site** dialog (see "Edit Site Dialog Box" on page 292).
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this SBC.
Postliminary	A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying the SBC.
Enabled	Lets you turn a postliminary on or off without deleting it.
Script	Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

"External SBC" on page 127

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

6

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

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 (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 in order for Conference Manager 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 152 and "MCU Pool Orders" on page 156.

Note

If you have a Polycom RealPresence Resource Manager system that uses the DMA system API to schedule conferences on the DMA system's conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for the use of the RealPresence Resource Manager system. The pool orders should be named in such a way that:

- They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
- Users of that system will understand that they should choose one of those pool orders.

If the RealPresence Resource Manager system is also going to directly schedule conferences on MCUs that it manages, those MCUs should not be part of the conferencing resources (MCU pools) available to the DMA system.

Note

MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing. See "ISDN Gateway Selection Process" on page 147.

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.

Note

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.

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.

Note

In order to efficiently manage multiple calls as quickly as possible, the Polycom DMA system uses multiple connections per MCU. By default, an RMX MCU allows up to 20 connections per user. We recommend not reducing this setting (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). If you have a DMA supercluster with three Conference Manager clusters and a busy conferencing environment, we recommend increasing this value to 30.

> **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 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.

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
	Connection and service status and capabilities:
	Connected Disconnected
	Connected securely (encrypted connection)
	In service Out of service
	Busied out Not licensed
	Supports conference recording
	Doesn't support conference recording
	Supports shared number dialing IVR service
	Functions as a gateway
	Supports SVC conferences (see "SVC Conferencing Support" on page 4)
	Warning
	Hover over an icon to see the associated status message.
Name	The name of the MCU.
Model	The type of MCU.
Version	The version of software on the MCU.

Table 6-1   *Information in the MCU list*

Column	Description
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	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).
	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).
	This feature is available only on RMX v. 6.0 or later MCUs and with a Polycom CMA system. It's not available for use with a Polycom RealPresence Resource Manager system, which can't share MCUs with the DMA system.
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.

Table 6-1   *Information in the MCU list*

Column	Description
Registration Status	The registration status of the device: • Active — The device is registered and can make and receive calls. • Inactive — The device's registration has expired. Whether it can make and receive calls depends on the system's rogue call policy (see "Call Server Settings" on page 239). It can register again. • Permanent — The device's registration never expires. • 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. • Quarantined (Inactive) — The device was quarantined, and its registration has expired. It can register again, returning to Quarantined status. • 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. A device's status can be determined by: • An action by the device. • An action applied to it manually on this page. • The expiration of a timer. • The application of a registration policy and admission policy (see "Registration Policy" on page 268).
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).
Site	The site in which the MCU is located. See "Sites" on page 285.

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 **Device Details** dialog box for the selected MCU.
Add	Opens the **Add MCU** dialog box, where you can add an MCU to the pool of devices known to the Polycom DMA system.

Table 6-2   *MCU commands*

Command	Description
Edit	Opens the **Edit MCU** 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 MCUs as conferencing resources or ISDN gateways (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 MCUs as conferencing resources or ISDN gateways. A dialog box asks you to confirm. If you do so, existing calls on the MCUs are terminated or (for SIP calls only) migrated to in-service MCUs with available capacity.
	If any of the MCUs are ISDN gateways, the system stops using them for simplified gateway dialing.
	This command immediately terminates the system's use of the MCUs as conferencing resources or ISDN gateways. It has no effect on the MCUs themselves, which continue to accept any calls from other sources.
Busy Out	Stops the Polycom DMA system from creating new conferences on the selected MCUs, but allows existing conferences to continue and accepts new calls to those conferences. A dialog box asks you to confirm.
	If any of the MCUs are ISDN gateways, the system stops using them 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 MCUs themselves, which continue to accept any calls from other sources.
Quarantine	Allows the selected MCUs to register (or remain registered), but not to make or receive calls.
	If the selected MCUs are quarantined, this becomes **Unquarantine**.
Block	Prevents the selected MCUs from registering.
	If he selected MCUs are blocked, this becomes **Unblock**.

> **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.
>
> If you have a Polycom CMA system and want to use the same RMX MCU (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 the CMA system. This feature is not available for Cisco Codian MCUs or for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.
>
> 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

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

> **Note**
>
> 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.
>
> 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.

> **Note**
>
> MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing. See "ISDN Gateway Selection Process" on page 147.
>
> 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
External MCU	
Name	Name for the MCU (up to 32 characters).
Type	Lists the types of MCUs the system supports. Must be set to the correct MCU type in order for the DMA system to be able to connect to it.
Management IP address	IP address for logging into the MCU (to use it as a conferencing resource).
Admin user 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 your Polycom CMA system to use for scheduled conferences (requires RMX v6.0 or later).
	Note: This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.

Table 6-3   Add MCU dialog box

Field	Description
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 your Polycom CMA system to use for scheduled conferences (requires RMX v6.0 or later).
	Note: This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.
Strip prefix	If selected, the DMA system strips the prefix when a call that includes a prefix is routed to this MCU.
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.
	Gateways don't need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the DMA system can choose from a pool of available gateways (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277).
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 the configuration of the Polycom DMA system and the MCU.

Table 6-3   *Add MCU dialog box*

Field	Description
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.
	Caution: Before adding an MCU to the DMA system's conferencing resources, make sure that MCU isn't already a RealPresence Resource Manager system conferencing resource. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences.
Enable gateway profiles	Makes the MCU available for selection as an ISDN gateway device and enables the **Gateway Profiles** tab for configuring gateway session profiles.
	Gateway session profiles indicate to the MCU the bandwidth parameters to be used for the ISDN connection. They can be used for:
	• ISDN gateway calls to the MCU's direct dial-in prefix. In this case, the caller specifies the session profile prefix in the dial string: `<direct dial-in prefix><session profile prefix><delimiter><E.164 number>`
	• Calls to simplified ISDN gateway dialing prefixes (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277). In this case, the DMA system selects the MCU/gateway and its session profile. See "ISDN Gateway Selection Process" on page 147.
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.
Permanent	Prevents the MCU's registration with the Call Server from ever expiring. For MCUs, this option should always be selected (the default).

Table 6-3   *Add MCU dialog box*

Field	Description
Gateway Profiles	
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 **Add** to add a session profile. Click **Edit** or **Delete** to change or delete the selected profile. You can't change or delete session profiles that the MCU/gateway registered with, only those that you added.
Media IP Addresses	
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 **Add** to add it the list below.
Media IP addresses	List of media addresses for the MCU.
	Click **Remove** to delete the selected address from the list.
Postliminary	A postliminary is an executable script, written in the Javascript language, that defines dial transformations to be applied before routing the call to the MCU/gateway.
Enabled	Lets you turn a postliminary on or off without deleting it.
Script	Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

"MCUs" on page 131

"MCU Procedures" on page 149

"Add Session Profile Dialog Box" on page 146

"Edit Session Profile Dialog Box" on page 146

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

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**
>
> 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.
>
> 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.

> **Note**
>
> MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing. See "ISDN Gateway Selection Process" on page 147.
>
> 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
External MCU	
Name	Name for the MCU (up to 32 characters).
Type	Lists the types of MCUs the system supports. Must be set to the correct MCU type in order for the DMA system to be able to connect to it.
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.

Table 6-4   *Edit MCU dialog box*

Field	Description
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 your Polycom CMA system to use for scheduled conferences (requires RMX v6.0 or later).
	Note: This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.
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 your Polycom CMA system to use for scheduled conferences (requires RMX v6.0 or later).
	Note: This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.
Strip prefix	If selected, the system strips the prefix when a call that includes a prefix is routed to this MCU.
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.
	Gateways don't need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the DMA system can choose from a pool of available gateways (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277).
Signaling address for H.323	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.
	Gateways don't need a direct dial-in prefix if you define simplified ISDN gateway dialing prefixes so that the DMA system can choose from a pool of available gateways (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277).

Table 6-4   *Edit MCU dialog box*

Field	Description
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 the configuration of the Polycom DMA system and the MCU.
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.
	Caution: Before adding an MCU to the DMA system's conferencing resources, make sure that MCU isn't already a RealPresence Resource Manager system conferencing resource. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences.
Enable gateway profiles	Makes the MCU available for selection as an ISDN gateway device and enables the **Gateway Profiles** tab for configuring gateway session profiles.
	Gateway session profiles indicate to the MCU the bandwidth parameters to be used for the ISDN connection. They can be used for:
	• ISDN gateway calls to the MCU's direct dial-in prefix. In this case, the caller specifies the session profile prefix in the dial string: `<direct dial-in prefix><session profile prefix><delimiter><E.164 number>`
	• Calls to simplified ISDN gateway dialing prefixes (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277). In this case, the DMA system selects the MCU/gateway and its session profile. See "ISDN Gateway Selection Process" on page 147.
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.

Table 6-4   Edit MCU dialog box

Field	Description
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.
Permanent	Prevents the MCU's registration with the Call Server from ever expiring. For MCUs, this option should always be selected (the default).
Gateway Profiles	
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 **Add** to add a session profile. Click **Edit** or **Delete** to change or delete the selected profile. You can't change or delete session profiles that the MCU/gateway registered with, only those that you added.
Media IP Addresses	
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 **Add** to add it the list below.
Media IP addresses	List of media addresses for the MCU. Click **Remove** to delete the selected address.
Postliminary	A postliminary is an executable script, written in the Javascript language, that defines dial transformations to be applied before routing the call to the MCU/gateway.
Enabled	Lets you turn a postliminary on or off without deleting it.
Script	Type (or paste) the postliminary script you want to apply. Then click **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries and test the script with various variables.

See also:

Add Session Profile Dialog Box

Lets you add a session profile prefix to the ISDN 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 H.323 PSTN SIP	Select the protocol(s) for this profile. Only H.320 and PSTN are relevant when adding a profile. The others are selected if the gateway specified them when registering.

See also:

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   Edit 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 137

"Edit MCU Dialog Box" on page 142

ISDN Gateway Selection Process

When the dial string begins with a simplified ISDN gateway dialing prefix, the Polycom DMA system chooses an ISDN gateway by applying the following steps:

1 Strip the ISDN gateway dialing prefix from the dial string, leaving the E.164 number.

2 From the in-service (not busied out or out of service) gateways, select the ones that have a profile with a matching or higher bit rate (higher bit rate can only be used for RMX). If none, go to 3; otherwise, go to 4.

3 From the remaining gateways, select those with a profile bit rate lower than the requested bit rate. If none, reject the call.

4 From the remaining gateways, select those that match the country code and area code of the dialed number. If none, go to 5; otherwise, go to 6.

5 From the remaining gateways, select those that match the country code of the dialed number, if any.

6 From the remaining gateways, select those with a profile that has the closest bit rate. An exact match is preferred.

7 From the remaining gateways, select those that are in the same site as the calling endpoint, if any.

8 From the remaining gateways, select one using a round-robin method.

9 If the call fails because of no capacity on the selected gateway, select the next gateway left in 8. If none, start again at 2 (omitting the gateway that failed). If none left, reject the call.

10 If a gateway is successfully selected, assemble a dial string to send to the gateway as follows:
```
<direct dial-in prefix><session profile prefix><delimiter><E.164
number>
```

See also:

MCU Procedures

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 137.

4   To set aside some of the MCU's capacity for the Polycom CMA system's use, set **Video ports reserved for CMA system** and **Voice ports reserved for CMA system** to the desired values (requires RMX v6.0 and above).

     The ports reserved for the Polycom CMA system can be used by that system for scheduled conferences.

Note

This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.

5   To use a gateway-capable MCU as an ISDN gateway, select the **Enable gateway profiles** check box and, on the **Gateway Profiles** 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 MCU 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 152.

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 156.

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 142.

6 To set aside more or fewer ports for the Polycom CMA system's use, change the **Video ports reserved for CMA system** and **Voice ports reserved for CMA system** values (requires RMX v6.0 and above).

> **Note**
>
> This feature is not for use with a Polycom RealPresence Resource Manager system. The RealPresence Resource Manager system must have exclusive use of any MCUs on which it directly schedules conferences. Those MCUs should not be added to the DMA system's conferencing resources.

7 To use a gateway-capable MCU as an ISDN gateway, select the **Enable gateway profiles** check box and, on the **Gateway Profiles** tab, specify a dial string delimiter and add or change session profiles. To stop using it, clear the **Enable gateway profiles** 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 152.

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 156.

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 one or more MCUs for conferencing and simplified ISDN dialing

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

2   In the **MCUs** list, select the MCUs of interest.

3   In the **Actions** list, select **Stop Using**.

4   When asked to confirm that you want to stop using the MCUs, click **Yes**.

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

This has no effect on the MCUs themselves, which continue to accept any calls from other sources.

To stop using one or more MCUs, but allow existing calls and conferences to continue

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

2   In the **MCUs** list, select the MCUs of interest.

3   In the **Actions** list, select **Busy Out**.

4   When asked to confirm that you want to busy out the MCUs, click **Yes**.

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

This has no effect on the MCUs themselves, which continue to accept any calls from other sources.

To start using one or more MCUs for conferencing and simplified ISDN dialing again

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

2   In the **MCUs** list, select the out-of-service MCUs of interest.

3   In the **Actions** list, select **Start Using**.

See also:

"MCUs" on page 131

"Add MCU Dialog Box" on page 137

"Edit MCU Dialog Box" on page 142

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.

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 156.

> **Note**
>
> If you have a Polycom RealPresence Resource Manager system that uses the DMA system API to schedule conferences on the DMA system's conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for the use of the RealPresence Resource Manager system. The pool orders should be named in such a way that:
>
> •   They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
>
> •   Users of that system will understand that they should choose one of those pool orders.
>
> If the RealPresence Resource Manager system is also going to be used to directly schedule conferences on MCUs, those MCUs should not be part of the conferencing resources (MCU pools) available to the DMA system.

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 **Add MCU Pool** dialog box, where you can define a new pool.
Edit	Opens the **Edit MCU Pool** 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

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:

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 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, enter a name and description, and select the MCUs to include in the pool. See "Add MCU Pool Dialog Box" on page 154.

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 154.

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 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.

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 329.

- 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 152.

> **Note**
>
> If you have a Polycom RealPresence Resource Manager system that uses the DMA system API to schedule conferences on the DMA system's conferencing resources (MCU pools), you must create MCU pools and pool orders specifically for the use of the RealPresence Resource Manager system. The pool orders should be named in such a way that:
>
> - They appear at the top of the pool order list presented in the RealPresence Resource Manager system.
>
> - Users of that system will understand that they should choose one of those pool orders.
>
> If the RealPresence Resource Manager system is also going to be used to directly schedule conferences on MCUs, those MCUs should not be part of the conferencing resources (MCU pools) available to the DMA system.

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 **Add MCU Pool Order** dialog box, where you can define a new pool order.
Edit	Opens the **Edit MCU Pool Order** 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

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 fall back to any available MCU if there are no available MCUs in its pools.

See also:

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 fall back to any available MCU if there are no available MCUs in its pools.

See also:

MCU Selection Process

> **Note**
>
> MCU pools and pool orders are not used to select an ISDN gateway for simplified gateway dialing. See "ISDN Gateway Selection Process" on page 147.
>
> The process below can be affected by the mechanisms that the system uses for detecting and handling MCU availability and reliability issues. See "MCU Availability and Reliability Tracking" on page 160.

The Polycom DMA system chooses an MCU for a user's conference by applying the following rules in order:

1 Select the MCU pool order:

a Use the pool order directly assigned to the user's conference room.

b If none, use the highest priority pool order associated with any group to which the user belongs.

c If none, use the system default.

2 Select the first MCU pool in the MCU pool order.

3 Select the best MCU in the MCU pool, based on how well their capabilities fulfill the user's needs in the following respects:

— MCU has 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, as determined by the following formula:

```
port_availability = (free_video_ports / total_video_ports) +
(0.0001 * free_audio_ports / total_audio_ports)

mixer_availability = (total_video_ports - 2 *
active_dma_conferences) / total_video_ports + 0.0001 *
(total_audio_ports - 2 * active_dma_conferences) /
total_audio_ports

availability = min (port_availability, mixer_availability)
```

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 in the pool order:

— 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.

See also:

MCU Availability and Reliability Tracking

In order to minimize the number of failed calls, the Polycom DMA system employs mechanisms for detecting and handling MCU availability and reliability issues:

• If it can't reach an MCU's management interface, the DMA system won't route calls to that MCU.

• If an MCU reports zero capacity via its management interface, the DMA system won't route calls to that MCU.

• When calls to a specific MCU fail, the DMA system reduces the MCU's reliability score, causing it to be selected less frequently than other MCUs.

An MCU's reliability depends on the number of consecutive failed calls. As that number increases, the DMA system treats a growing percentage of the MCU's ports as if they were in use. Since the DMA system selects the least used of the capable MCUs in its pool, the likelihood that an MCU with failures will be chosen for the next call declines rapidly (depending on the number of consecutive failed calls and the remaining capacity in the MCU pool).

Table 6-15 *How failed calls reduce the apparent capacity of an MCU*

Consecutive Failed Calls	Percentage of Ports Assumed To Be in Use
1	24%
2	43%
3	56%
4	67%
5	74%
6	80%

Table 6-15   How failed calls reduce the apparent capacity of an MCU (continued)

Consecutive Failed Calls	Percentage of Ports Assumed To Be in Use
7	84%
8	88%
9	90%

Every 30 minutes, the reliability score of the MCU is increased so that it won't be permanently removed from the pool due to failures in the distant past. To avoid trying the MCU every 30 minutes, monitor the DMA system and administratively take the MCU out of service.

By increasing the number of MCUs in the pool or increasing their capacity, you can decrease the usage of the working MCUs during a failover scenario. So, for example, if you want to avoid routing any more calls to an MCU after two consecutive failed calls, provide enough excess capacity that the remaining MCUs never all reach 43% port usage during a failure.

> **Note**
>
> After each call, the DMA system recalculates the reliability of an MCU as the weighted average of the result for the current call (1 for success, 0 for failure) and the reliability of all previous calls, using this formula:
>
> ```
> reliability = (current_call + (weight * previous_reliability)) /
> (1 + weight)
> ```
>
> For example, if weight is 5, previous reliability is 1 (no previous failed calls), and the call is sucessful, the reliability remains 1:
>
> ```
> (1 + (5 *1)) / (1 + 5) = 1
> ```
>
> If weight is 5, previous reliability is 1, and the call fails, the reliability becomes 5/6:
>
> ```
> (0 + (5 *1)) / (1 + 5) = 5/6
> ```
>
> If weight is 5, previous reliability is 5/6, and the call is successful, the reliability becomes 31/36:
>
> ```
> (1 + (5 *5/6)) / (1 + 5) = 31/36
> ```
>
> If the reliability is ever less than 1, it exponentially approaches 1 as more calls succeed, but it never quite gets there. It very quickly reaches the point where the weight of the past failed call counts less than a single call in progress. But it remains as the tie breaker between completely unused MCUs forever.

See also:

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 154.

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 154.

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:

7

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
- Resource Management 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 daily, 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 or Office Communications Server integrations. Please see 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

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

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

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

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

Field	Description
Domain\user name	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.
	Note: 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.
	The Polycom DMA system initially assigns the Administrator user role to this user (see "User Roles Overview" on page 312), so you can use this account to give administrative access to other enterprise user accounts.
	Caution: Leaving a user role assigned to this account represents a *serious security risk.* For best security, remove the Administrator user role so that it can't be used for logging into the Polycom DMA system management interface.
Password	Login password for service account user ID.
User LDAP filter	Specifies which user accounts to include (an underlying, non-editable filter excludes all non-user objects in the directory). The default expression includes all users that don't have a status of disabled in the directory.
	Don't edit this expression unless you understand LDAP filter syntax. See RFC 2254 for syntax information.
Base DN	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 "Understanding Base DN" on page 173.
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	Specifies the territory whose Polycom DMA system cluster is responsible for updating the user and group data cache.
	In a superclustered system, this information is shared across the supercluster. The other clusters access the directory only to authenticate passwords. See "Territories" on page 302 for more information.

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

Field	Description
Enterprise Conference Room ID Generation	
Directory attribute	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.
	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.
	Leave this field blank if you don't want the system to create conference rooms for the enterprise users.
Characters to remove	Characters that might need to be stripped from a phone number field's value to ensure a numeric conference room ID.
	The default string includes **\t**, which represents the tab character. Use **** to remove backslash characters.
	If generating alphanumeric conference room IDs, remove the following:
	()&%#@|"':;,
	Single spaces in the source field are preserved, but multiple consecutive spaces are concatenated to one space.
Maximum characters used	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.
Enterprise Chairperson and Conference Passcode Generation	
Chairperson directory attribute	The name of the Active Directory attribute that contains the chairperson passcodes. In choosing an attribute, remember that passcodes must be numeric.
	The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. But if the attribute isn't in the Global Catalog, the system queries each domain controller for the data.
	Leave this field blank if you don't want the system to create chairperson passcodes for the enterprise users.
Maximum characters used	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.

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

Field	Description
Conference directory attribute	The name of the Active Directory attribute that contains the conference passcodes. In choosing an attribute, remember that passcodes must be numeric.
	The attribute must be in the Active Directory schema and preferably should be replicated across the enterprise via the Global Catalog server mechanism. But if the attribute isn't in the Global Catalog, the system queries each domain controller for the data.
	Leave this field blank if you don't want the system to create conference passcodes for the enterprise users.
Maximum characters used	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.

See also:

"Microsoft Active Directory Integration" on page 163

Active Directory Integration Procedure

Before performing the procedure below, read "Set Up Security" on page 28 and "Connect to Microsoft Active Directory" on page 32. You should also have a good idea of how many enterprise users you expect the system to retrieve.

To integrate with Active Directory

> **Note**
>
> Unless the **Allow unencrypted connections to the Active Directory** security option is enabled (see "Security Settings" on page 48), the Polycom DMA system offers the same SSL server certificate that it offers to browsers connecting to the system management interface. The Microsoft Active Directory server must be configured to trust the certificate authority.

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 RealPresence Resource Manager or CMA system, be aware that the machine account used for AD integration by the RealPresence Resource Manager or 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 RealPresence Resource Manager or CMA system is allowed to log into should contain only the RealPresence Resource Manager or 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 333.

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 174.

---

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 173.

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**, clear the **Local users only** check box, locate your named enterprise account, and give it Administrator privileges. See "User Roles Overview" on page 312 and "Users Procedures" on page 333.

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 320.

> **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 7.

    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 163

"Adding Passcodes for Enterprise Users" on page 174

"Active Directory Integration Report" on page 418

"Conference Room Errors Report" on page 422

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.

Use this Base DN:	To include the following:
All Domains	0-11
DC=nwind,DC=com	0-10
DC=nwind,DC=net	11
DC=eng,DC=nwind,DC=com	1-5
DC=mkt,DC=nwind,DC=com	6-8
DC=fin,DC=nwind,DC=com	9 & 10
DC=west,DC=eng,DC=nwind,DC=com	2
DC=east,DC=eng,DC=nwind,DC=com	3-5
OU=Planning,DC=fin,DC=nwind,DC=com	10
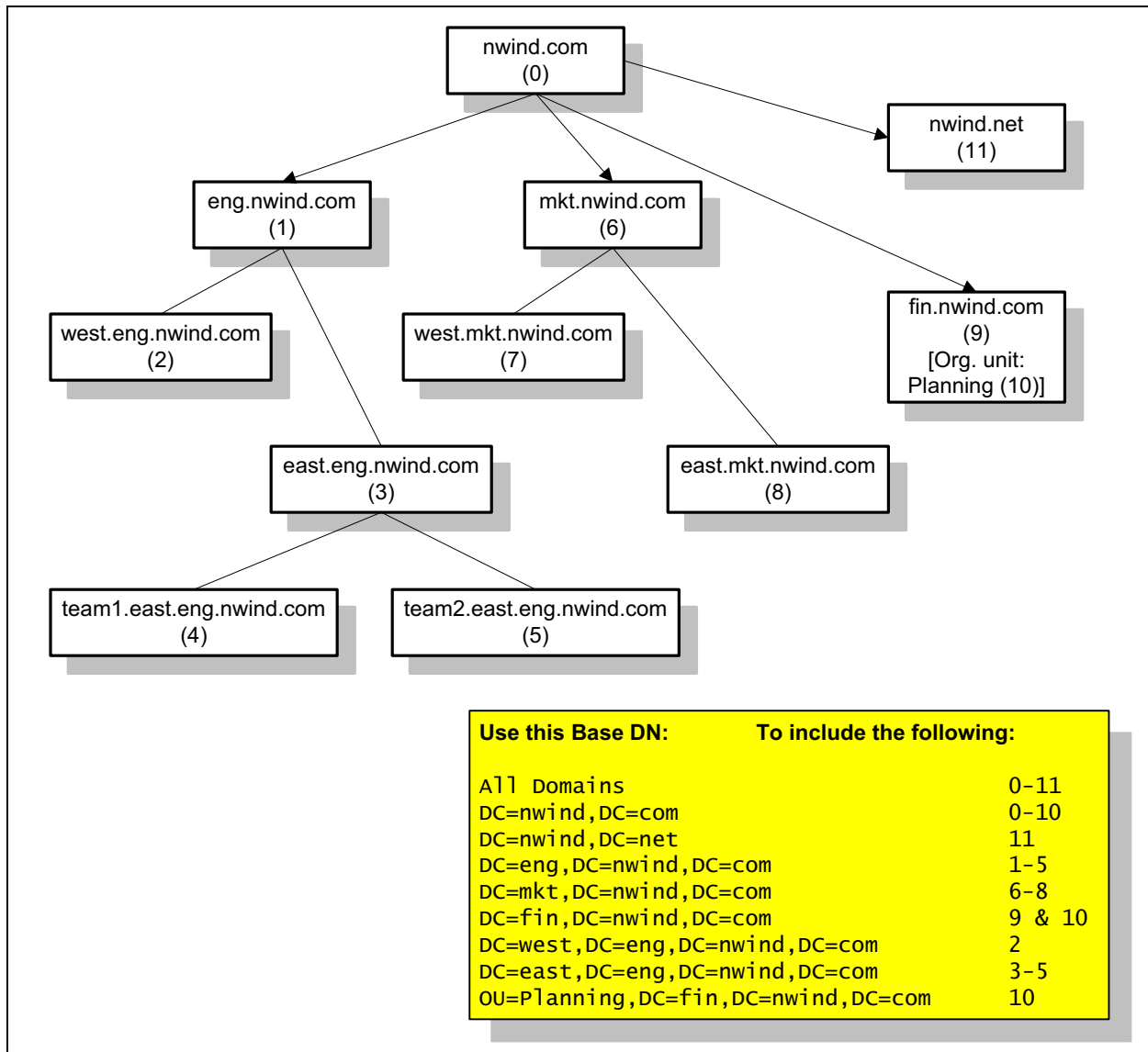
The **Base DN** field defaults to *All Domains* (which is equivalent to specifying an empty base DN in a query). Initially, the only other option is to enter a custom DN value. The first time you tell the system to connect to the Active Directory server, leave **Base DN** set to *All Domains*.

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:

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 200).

> **Note:**
>
> If Cisco 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:

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 173.

- 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 163.

- 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 163 and "Adding Passcodes for Enterprise Users" on page 174.

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 173.

- 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 173.

- 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 418.

- 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 173.

- 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 163. 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 163.

- 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 163

"Microsoft Active Directory Page" on page 165

"Active Directory Integration Procedure" on page 169

"Understanding Base DN" on page 173

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.

When you integrate the DMA system with an Exchange server, it connects to the Exchange server as the Polycom Conferencing user and subscribes to notifications. The Exchange server notifies the DMA system as soon as a meeting invitation (or other mail) arrives in the Polycom Conferencing user inbox. It also sends heartbeat messages to verify that the subscription is working.

If the DMA system fails to receive a heartbeat or other notification for 30 seconds, it begins checking its inbox every four minutes for new messages, and also attempts to reestablish the subscription (push connection) each time.

> **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 Office Communications Server integrations. Please see 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 54.

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, Polycom m100, 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 accepts or declines these invitations. A meeting invitation is declined if:

- The VMR number is in use by any other conference room (calendared, enterprise, or custom).

- The user sending the invitation 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 193).

- The conference or chairperson passcode is not valid (see "Adding Passcodes for Enterprise Users" on page 174).

> **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.
>
> 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 163

"Microsoft Exchange Server Page" on page 182

"Exchange Server Integration Procedure" on page 183

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 **Update** 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.

Table 7-2   *Fields on the Microsoft Exchange Server page (continued)*

Field	Description
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 "Territories" on page 302 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 180

"Exchange Server Integration Procedure" on page 183

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 48), 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 in order for the DMA system to subscribe to notifications.

If he DMA system is unable to subscribe to notifications, the Microsoft Exchange Server status (see Dashboard) remains **Subscription pending** indefinitely and the Polycom DMA system doesn't automatically receive calendar notifications. Instead, it must check the Polycom Conferencing mailbox for meeting request messages, which it does every 4 minutes.

1 Confirm that the Polycom DMA system has been successfully integrated with your Active Directory (see "Integrations with Other Systems" on page 163) 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:

Resource Management System Integration

Integrating with a resource management system (either a Polycom RealPresence Resource Manager system or a Polycom CMA system) provides the Polycom DMA system with:

- All site topology information configured in the RealPresence Resource Manager or CMA system.

- All user-to-device associations configured in the RealPresence Resource Manager or CMA system.

The Polycom DMA system uses site topology information for a variety of purposes, including cascading of conferences, bandwidth management, Session Border Controller selection. See "Add Conference Template Dialog Box" on page 200 and "About the Call Server Capabilities" on page 238.

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 101.

If you have a Polycom RealPresence Resource Manager or CMA system, integrating with it allows you to configure site topology and user-to-device associations in one place instead of two, ensuring consistency.

If you don't have a Polycom RealPresence Resource Manager or CMA system (or for some reason don't want to integrate with it), both kinds of information can be manually configured on the Polycom DMA system.

> **Note**
>
> A RealPresence Resource Manager system (but not a CMA system) can be integrated with (connected to) the DMA system. This enables it to use the DMA system's RealPresence Platform API to set up and monitor scheduled and preset dial-out (*anytime*) conferences using the DMA system's resources (see "RealPresence Platform API" on page 3).
>
> When you integrate a RealPresence Resource Manager system with the DMA system (from its management interface), the DMA system is automatically integrated back to the RealPresence Resource Manager system (the integration described here).

While the Polycom DMA system is integrated with the Polycom RealPresence Resource Manager or CMA system, site topology and user-to-device association may only be configured on the Polycom RealPresence Resource Manager or CMA system. If the integration is terminated, the Polycom DMA system retains the information last obtained from the RealPresence Resource Manager or CMA system, but it becomes editable.

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 24.

In addition, the DNS servers must be able to resolve the Polycom RealPresence Resource Manager or CMA system's FQDN to its IP address. This is necessary even if you specify the Polycom RealPresence Resource Manager or CMA system's IP address when you join it.

> **Note**
>
> RealPresence Resource Manager or CMA integration is not supported in **Maximum security** mode. See "The Consequences of Enabling Maximum Security Mode" on page 54.
>
> If you want to support cascading, but don't have a Polycom RealPresence Resource Manager or CMA system, you must create site topology information on the Polycom DMA system. See "Site Topology" on page 283.
>
> 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:

Resource Management System Page

The **Resource Management System** page contains the **Join Resource Management System** command, which you use to integrate with your Polycom RealPresence Resource Manager or CMA system. When the system is integrated with a Polycom RealPresence Resource Manager or CMA system, it contains the **Leave Resource Management System** command, which you use to terminate the integration.

> **Note**
>
> A RealPresence Resource Manager system (but not a CMA system) can be integrated with (connected to) the DMA system. This enables it to use the DMA system's RealPresence Platform API to set up and monitor scheduled and preset dial-out (*anytime*) conferences using the DMA system's resources (see "RealPresence Platform API" on page 3).
>
> When you integrate the RealPresence Resource Manager system with the DMA system (from its management interface), the DMA system is automatically integrated back to the RealPresence Resource Manager system (the integration described here).

The list on this page displays information about the Polycom RealPresence Resource Manager or CMA system. The following table describes the fields in the list.

Table 7-3   Fields in the Resource Management System list

Field	Description
Host name	Name of the system.
IP Address	IP address of the system.
Model	Type of system.
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:

Join Resource Management System Dialog Box

Lets you integrate the Polycom DMA system with a Polycom RealPresence Resource Manager or CMA system to obtain site topology information and user-to-device association information.

> **Note**
>
> RealPresence Resource Manager or CMA integration is not supported in **Maximum security** mode. See "The Consequences of Enabling Maximum Security Mode" on page 54.

> **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 24.
>
> In addition, the DNS servers must be able to resolve the Polycom RealPresence Resource Manager or CMA system's FQDN to its IP address. This is necessary even if you specify the Polycom RealPresence Resource Manager or 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 Resource Management System dialog box*

Field	Description
Host name or IP address	The Polycom RealPresence Resource Manager or CMA system with which to integrate.
User name	Administrative user ID with which the Polycom DMA system can log into the Polycom RealPresence Resource Manager or CMA system.
Password	Password for the administrative user ID.

See also:

"Integrations with Other Systems" on page 163

"Resource Management System Integration" on page 185

"Resource Management System Page" on page 186

"Resource Management System Integration Procedures" on page 188

Resource Management System Integration Procedures

Note

RealPresence Resource Manager or CMA integration is not supported in **Maximum security** mode. See "The Consequences of Enabling Maximum Security Mode" on page 54.

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 24.

In addition, the DNS servers must be able to resolve the Polycom RealPresence Resource Manager or CMA system's FQDN to its IP address. This is necessary even if you specify the Polycom RealPresence Resource Manager or CMA system's IP address when you join it.

To integrate with a resource management system

1   Go to **Admin > Integrations > Resource Management System**.

2   In the **Actions** list, select **Join Resource Management System**.

3   In the **Join Resource Management System** dialog box, enter the host name or IP address of the Polycom RealPresence Resource Manager or 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 RealPresence Resource Manager or 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 **Resource Management System** page, verify the 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 RealPresence Resource Manager or CMA system.

To terminate the integration with a resource management system

1 Go to **Admin > Integrations > Resource Management System**.

2 In the **Actions** list, select **Leave Resource Management System**.

3 When asked to confirm that you want to leave, click **Yes**.

The system connects to the Polycom RealPresence Resource Manager or CMA system and terminates the integration. A dialog box informs you when the process is complete.

4 On the **Resource Management System** page, verify that the system is no longer integrated with the Polycom RealPresence Resource Manager or CMA system.

The Polycom DMA system retains the site topology and user-to-device association information last obtained from the RealPresence Resource Manager or CMA system, but it's now editable.

See also:

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. This allows the DMA system to consult a configured policy on the Juniper SRC system at call time to assure and/or reserve required network resources for a call. It also allows priority and preemption policies to be applied to DMA system calls.

In addition, the DMA system's priority-based QoS packet marking (Gold/Silver/Bronze class of service) is applied by the Juniper SRC system throughout the network it controls.

See also:

"Integrations with Other Systems" on page 163

"Juniper Networks SRC Page" on page 190

"Juniper Networks SRC Integration Procedure" on page 191

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 **Update** 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.
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: 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.

See also:

"Juniper Networks SRC Integration" on page 189

"Juniper Networks SRC Integration Procedure" on page 191

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:

8

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	E.164 dial string prefix for calling the system. 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. 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. **Caution:** Changing the dialing prefix terminates any existing H.323 calls. When you click **Update**, the system prompts you to confirm.
Default max total participants	Specifies the maximum conference size assigned to a conference room if a larger or smaller maximum size isn't specified for it. **Automatic** (the default setting) uses the largest conference size supported by the MCU as the default maximum.
Default conference template	Default template used by the system. See "Conference Templates" on page 195.
Default territory	The territory assigned to a user's conference room if it isn't specified at the user or conference room level. 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.
Default MCU pool order	Default MCU pool order used by the system. See "MCU Pool Orders" on page 156.
Minimum and maximum generated room ID	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. The six-digit limit applies only to generated IDs for custom conference rooms.
Conference Duration	Default maximum duration of a conference (in hours and minutes) or **Unlimited** (the maximum in this case depends on the MCU).

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 195

"Shared Number Dialing" on page 221

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**
>
> The Polycom DMA system supports the use of Cisco 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 152 and "MCU Pool Orders" on page 156). 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 152 and "MCU Pool Orders" on page 156.

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 152 and "MCU Pool Orders" on page 156.

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 152 and "MCU Pool Orders" on page 156). 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 193). 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 195

"Template Priority" on page 197

"About Conference IVR Services" on page 197

"About Cascading" on page 198

"Conference Templates Procedures" on page 220

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 195

"Two Types of Templates" on page 195

"About Conference IVR Services" on page 197

"About Cascading" on page 198

"Conference Templates Procedures" on page 220

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 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:

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 RealPresence Resource Manager or CMA system in your network, you can enable cascaded conferences with these steps:

1   On the Polycom RealPresence Resource Manager or 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 RealPresence Resource Manager or CMA system to obtain its site topology data. See

3 On the Polycom DMA system, enable cascading in some or all of your conference templates.

If you don't have a Polycom RealPresence Resource Manager or CMA system, you must define your site topology in the Polycom DMA system instead of importing it. See "Site Topology" on page 283.

> **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 156.

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):

• If the caller is in a site that contains one or more MCUs, the system selects an MCU in that site that has available capacity.

• If the caller is in a site that doesn't contain MCUs, the system looks for MCUs in directly-connected sites (that is, sites that have a network path to the caller's site without going through a cloud) and selects one that has available capacity.

If the selected 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 195

"Two Types of Templates" on page 195

"Template Priority" on page 197

"About Conference IVR Services" on page 197

"Conference Templates Procedures" on page 220

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 that template and create additional templates.

See also:

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 **Cisco Codian** section appears only if the system is licensed to use Cisco 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
Common Settings	
Name	A meaningful name for the template (up to 50 characters).
Description	A brief description of the conference template (up to 50 characters).

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
Conference mode	One of the following: • *AVC only* — Standard videoconferencing mode supporting the H.264 Advanced Video Coding (AVC) compression standard. In an AVC conference, the MCU transcodes the video stream to each device in the conference to provide an optimal experience, based on its capabilities. This is the only mode that supports the use of RMX profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs. • *SVC only* — Videoconferencing mode supporting the Annex G extension of the H.264 standard, known as H.264 Scalable Video Coding (SVC). An SVC video stream consists of a base layer that encodes the lowest available quality representation plus optional enhancement layers that each provide an additional quality improvement. The number of enhancement layers and the number of participants' video included in a video stream to a device can be tailored to fit the bandwidth available and device capabilities. SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC. Selecting this setting disables most of the other template settings. See "SVC Conferencing Support" on page 4.
RMX General Settings	
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 "Conference Templates" on page 195.
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 Cisco 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	Enables conferences using this template to span RMX MCUs. Cascading requires site topology information, which the Polycom DMA system can get from a Polycom RealPresence Resource Manager or CMA system (see "Resource Management System Integration" on page 185) or you can create (see "Site Topology" on page 283). See "About Cascading" on page 198 for more information about enabling cascading of conferences.
Video switching (VSW)	Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker). If this mode is enabled: • The minimum line rate available is 768 kbps (except for SD resolution, available only on RMX v7 MCUs with MPM+ or MPMx cards). • All endpoints must connect at the same line rate, and those that don't support the specified line rate are connected in voice-only mode. • The video clarity, layout, and skins settings are not available. • LPR is automatically turned off, but can be turned back on. If this option is 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.
H.264 high profile	Sets a VSW conference to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode). 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.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
Resolution	Available only if **Video switching** is selected. Offers the following resolution settings: • H.264 720p30 • H.264 1080p30 (available only on RMX MCUs with MPM+ or MPMx cards) • H.264 SD 30 (available only on RMX v7 MCUs with MPM+ or MPMx cards) • H.264 720p60 (available only on RMX v7 MCUs with MPM+ or MPMx cards) • H.264 CIF (available only on RMX v7 MCUs) • H.263 CIF (available only on RMX v7 MCUs) • H.261 CIF (available only on RMX v7 MCUs) • HD_720_P_30
Line rate	The maximum bit rate at which endpoints can connect to conferences using this template. If **Video switching** 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).
Encryption	Specifies the media encryption setting for conferences using this template: • No encryption — All endpoints join unencrypted. • Encrypt when possible — Endpoints supporting encryption join encrypted; others join unencrypted. • Encrypt all — Endpoints supporting encryption join encrypted; others can't join. **Note:** Prior to v7.2, RMX MCUs supported only encryption settings of On and Off. If an RMX running an older version is selected for a conference, the settings Encrypt when possible or Encrypt all are both converted to On. Consult the *Polycom RMX 1500/2000/4000 Administrator's Guide* for the version in question for detailed information about media encryption.
LPR	Enables *Lost Packet Recovery* for conferences using this template. LPR creates additional packets containing recovery information that can be used to reconstruct packets lost during transmission.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
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.
RMX Gathering Settings	
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 *RMX Administrator's Guide* to see an example of the slide and the location and appearance of these fields.
Info2	
Info3	
	On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint.
RMX Video Quality	
Video quality	Offers two video optimizations:
	• Motion — higher frame rate
	• Sharpness — higher resolution
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 **Video switching** is selected.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
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: • Graphics — lowest bit rate for basic graphics • High-resolution graphics — higher bit rate for better graphics resolution • Live video — the Content channel is used for live video A higher bit rate for the Content channel reduces the bit rate for the People channel.
Content protocol	Content channel protocol options: • Use H.263. • Use H.264 if available, otherwise use H.263. • Use H.264 cascade and SVC optimized. • Use H.264 HD.
RMX Video Settings	
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 **Video switching** or **Same layout** is selected, or if **Telepresence mode** 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 **Video switching** or **Same layout** is selected, or if **Telepresence mode** is Yes.
Same layout	Forces the selected layout on all participants. Personal selection of the video layout is disabled. Not available if **Presentation mode** or **Video switching** is selected, or if **Telepresence mode** 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 **Same layout** is selected or **Telepresence mode** is Yes.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
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 **Video switching** is selected or **Telepresence mode** is Yes.
Layout	With **Auto layout** deselected, this opens the **Select Layout** 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 "Select Layout Dialog Box" on page 219. Not available if **Video switching** is selected.
Telepresence mode	Support for telepresence conference rooms joining the conference: • Auto (default) — A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins. • Yes — Telepresence mode is on, regardless of whether a telepresence endpoint is present. • No — Telepresence mode is off, regardless of whether a telepresence endpoint is present. Available only on RMX v. 6.0 or later MCUs that are licensed for telepresence mode. We recommend always using Auto. **Note:** The RMX system flag ITP_CERTIFICATION must be set to YES. See the information about manually added system flags in the *Polycom RMX Administrator's Guide*.
Telepresence layout mode	Layout choices for telepresence conferences: • Manual — Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface. • Continuous Presence — Tells the MLA to generate a multipoint view (standard or custom). • Room Switch — Tells the MLA to use Voice Activated Room Switching (VARS). The speaker's site is the only one seen by others. Not available if **Telepresence mode** is No. See the *Polycom Multipoint Layout Application User Guide* for more information about layouts.
RMX Audio Settings	
Echo suppression	Enables the MCU to detect and suppress echo. Available only on MCUs with MPM+ or MPMx cards.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
Keyboard suppression	Enables the MCU to detect and suppress keyboard noise. Available only on MCUs with MPM+ or MPMx cards.
Audio clarity	Improves the voice quality in conference of a PSTN endpoint. Available only on RMX v7 MCUs.
RMX Skins	Lets you choose the display appearance (skin) for conferences using this template. Not available if **Telepresence mode** is Yes. or **Video switching** is enabled.
RMX Conference IVR	
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 "Adding Passcodes for Enterprise Users" on page 174. But you can override the Active Directory value; see "Edit User Dialog Box" on page 320. For local users, you can add or change chairperson passcodes when you create or edit the users. See "Edit User Dialog Box" on page 320.

Table 8-3   *Add Conference Template dialog box (continued)*

Field	Description
RMX Recording	
Record conference	The conference recording setting for this template:
	• Disabled — Recording isn't available for conferences using this template.
	• Immediately — Recording starts automatically when the conference starts.
	• Upon Request — Recording can be initiated manually by the chairperson or an operator.
	Conference recording requires a Polycom RSS recording system and an MCU that supports recording.
Recording link	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.
Audio only	Limits recording to the audio channel of the conference.
Indication of recording	Displays a red dot recording indicator in the upper left corner of the video layout.
	Available only on RMX v7.1 MCUs.
Cisco Codian	
Floor and chair control	Specifies how much control conference participants may have:
	• Do not allow — Participants have no control.
	• Floor only — A participant may "take the floor." Everyone sees that participant's video full-screen.
	• 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.
	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.
Automatic lecture mode	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.

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: • When used for MCU control • Always • Never 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 **Allow all resolutions** 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 **Select Layout** 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 "Select Layout Dialog Box" on page 219.

See also:

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 **Cisco Codian** section appears only if the system is licensed to use Cisco 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
Common Settings	
Name	A meaningful name for the template (up to 50 characters).
Description	A brief description of the conference template (up to 50 characters).
Conference mode	One of the following:
	• *AVC only* — Standard videoconferencing mode supporting the H.264 Advanced Video Coding (AVC) compression standard.
	This is the only mode that supports the use of RMX profiles, third-party and legacy endpoints, and Codian and legacy RMX MCUs.
	• *SVC only* — Videoconferencing mode supporting the Annex G extension of the H.264 AVC standard, known as H.264 Scalable Video Coding (SVC). An SVC video stream consists of a base layer that encodes the lowest available quality representation plus enhancement layers that each provide an additional quality improvement.
	The number of enhancement layers and the number of participants' video included in a video stream to a device can be tailored to fit the bandwidth available and device capabilities.
	SVC conferencing is only possible with Polycom RMX MCUs and Polycom endpoints that support H.264 SVC. Selecting this setting disables most of the other template settings.
	See "SVC Conferencing Support" on page 4.
RMX General Settings	
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 "Conference Templates" on page 195.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
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 Cisco 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 RealPresence Resource Manager or CMA system (see "Resource Management System Integration" on page 185) or you can create (see "Site Topology" on page 283). See "About Cascading" on page 198 for more information about enabling cascading of conferences.
Video switching (VSW)	Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker). If this mode is enabled: • The minimum line rate available is 768 kbps (except for SD resolution, available only on RMX v7 MCUs with MPM+ or MPMx cards). • All endpoints must connect at the same line rate, and those that don't support the specified line rate are connected in voice-only mode. • The video clarity, layout, and skins settings are not available. • LPR is automatically turned off, but can be turned back on. If this option is 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.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
H.264 high profile	Sets a VSW conference to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode).
	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.
Resolution	Available only if **Video switching** is selected. Offers the following resolution settings:
	• H.264 720p30
	• H.264 1080p30 (available only on RMX MCUs with MPM+ or MPMx cards)
	• H.264 SD 30 (available only on RMX v7 MCUs with MPM+ or MPMx cards)
	• H.264 720p60 (available only on RMX v7 MCUs with MPM+ or MPMx cards)
	• H.264 CIF (available only on RMX v7 MCUs)
	• H.263 CIF (available only on RMX v7 MCUs)
	• H.261 CIF (available only on RMX v7 MCUs)
	• HD_720_P_30
Line rate	The maximum bit rate at which endpoints can connect to conferences using this template.
	If **Video switching** is selected, the lowest line rate available depends on the **Resolution** setting chosen.
Encryption	Specifies the media encryption setting for conferences using this template:
	• No encryption — All endpoints join unencrypted.
	• Encrypt when possible — Endpoints supporting encryption join encrypted; others join unencrypted.
	• Encrypt all — Endpoints supporting encryption join encrypted; others can't join.
	Note: Prior to v7.2, RMX MCUs supported only encryption settings of On and Off. If an RMX running an older version is selected for a conference, the settings Encrypt when possible or Encrypt all are both converted to On.
	Consult the *Polycom RMX 1500/2000/4000 Administrator's Guide* for the version in question for detailed information about media encryption.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
LPR	Enables *Lost Packet Recovery* 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.
RMX Gathering Settings	
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 *RMX Administrator's Guide* to see an example of the slide and the location and appearance of these fields.
Info2	
Info3	
	On a 16:9 endpoint, a maximum of 96 characters can be displayed for each field, and fewer on a 4:3 endpoint.
RMX Video Quality	
Video quality	Offers two video optimizations:
	• Motion — higher frame rate
	• Sharpness — higher resolution
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.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
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 **Video switching** 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: • Graphics — lowest bit rate for basic graphics • High-resolution graphics — higher bit rate for better graphics resolution • Live video — the Content channel is used for live video A higher bit rate for the Content channel reduces the bit rate for the People channel.
Content protocol	Content channel protocol options: • Use H.263. • Use H.264 if available, otherwise use H.263. • Use H.264 cascade and SVC optimized. • Use H.264 HD.
RMX Video Settings	
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 **Video switching** or **Same layout** is selected, or if **Telepresence mode** 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 **Video switching** or **Same layout** is selected, or if **Telepresence mode** is Yes.
Same layout	Forces the selected layout on all participants. Personal selection of the video layout is disabled. Not available if **Presentation mode** or **Video switching** is selected, or if **Telepresence mode** is Yes.

Table 8-4   Edit Conference Template dialog box (continued)

Field	Description
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 **Same layout** is selected or **Telepresence mode** 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 **Video switching** is on or **Telepresence mode** is Yes.
Layout	With **Auto layout** deselected, this opens the **Select Layout** 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 "Select Layout Dialog Box" on page 219.
	Not available if **Video switching** is on.
Telepresence mode	Support for telepresence conference rooms joining the conference:
	• Auto (default) — A conference is automatically put into telepresence mode when a telepresence endpoint (RPX, TPX, ATX, or OTX) joins.
	• Yes — Telepresence mode is on, regardless of whether a telepresence endpoint is present.
	• No — Telepresence mode is off, regardless of whether a telepresence endpoint is present.
	Available only on RMX v. 6.0 or later MCUs that are licensed for telepresence mode. We recommend always using Auto.
	Note: The RMX system flag ITP_CERTIFICATION must be set to YES. See the information about manually added system flags in the *Polycom RMX Administrator's Guide*.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
Telepresence layout mode	Layout choices for telepresence conferences: • Manual — Layout is controlled manually by a conference operator using the Multipoint Layout Application (MLA) interface. • Continuous Presence — Tells the MLA to generate a multipoint view (standard or custom). • Room Switch — Tells the MLA to use Voice Activated Room Switching (VARS). The speaker's site is the only one seen by others. Not available if **Telepresence mode** is No. See the *Polycom Multipoint Layout Application User Guide* for more information about layouts.
RMX Audio Settings	
Echo suppression	Enables the MCU to detect and suppress echo. Available only on MCUs with MPM+ or MPMx cards.
Keyboard suppression	Enables the MCU to detect and suppress keyboard noise. Available only on MCUs with MPM+ or MPMx cards.
Audio clarity	Improves the voice quality in conference of a PSTN endpoint. Available only on RMX v7 MCUs.
RMX Skins	Lets you choose the display appearance (skin) for conferences using this template. Not available if **Telepresence mode** is Yes. or **Video switching** is enabled.
RMX Conference IVR	
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.

Table 8-4   Edit Conference Template dialog box (continued)

Field	Description
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 "Adding Passcodes for Enterprise Users" on page 174. But you can override the Active Directory value; see "Edit User Dialog Box" on page 320.
	For local users, you can add or change chairperson passcodes when you create or edit the users. See "Edit User Dialog Box" on page 320.
RMX Recording	
Record conference	The conference recording setting for this template:
	• Disabled — Recording isn't available for conferences using this template.
	• Immediately — Recording starts automatically when the conference starts.
	• Upon Request — Recording can be initiated manually by the chairperson or an operator.
	Conference recording requires a Polycom RSS recording system and an MCU that supports recording.
Recording link	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.
Audio only	Limits recording to the audio channel of the conference.
Indication of recording	Displays a red dot recording indicator in the upper left corner of the video layout.
	Available only on RMX v7.1 MCUs.

Table 8-4   *Edit Conference Template dialog box (continued)*

Field	Description
Cisco Codian	
Floor and chair control	Specifies how much control conference participants may have: • Do not allow — Participants have no control. • Floor only — A participant may "take the floor." Everyone sees that participant's video full-screen. • 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. 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.
Automatic lecture mode	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.
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: • When used for MCU control • Always • Never 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.

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 **Allow all resolutions** 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 **Select Layout** 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 "Select Layout Dialog Box" on page 219.

See also:

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 Codian MCU, select the layout you want.

3 Click **OK**.

See also:

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 200.

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

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:

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 *12345*, or *Direct Dial*.
Dial-In #	The complete dial string, for this VEQ. For instance, if the system uses the prefix 71, this might be *7112345*.
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 223

"Add Direct Dial Virtual Entry Queue Dialog Box" on page 224

"Edit Virtual Entry Queue Dialog Box" on page 225

"Edit Direct Dial Virtual Entry Queue Dialog Box" on page 225

"Conference Templates" on page 195

"Conference Settings" on page 193

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.
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:

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 *Direct Dial - English*.
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:

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:

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 *Direct Dial - English*.
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:

9

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 systems (either single-server or two-server systems) in distributed locations can be combined into a *supercluster*.

A supercluster is a set of up to 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, endpoint registrations, usage reporting, and status monitoring. Sharing and replicating this data also allows single-point management (configuration/re-configuration) of the shared data from any cluster of the supercluster. Up to three clusters can function as 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.

A standalone (not superclustered) Polycom DMA system has a single default territory for which it's the primary cluster (and of course there is no backup). When you join other clusters to it to create a supercluster, it still has that same single default territory, it's still the primary cluster for the default territory, and there is still no backup cluster. Essentially, one cluster is responsible for everything, and the others do nothing. So immediately after forming a new supercluster, you should do the following:

1   If you haven't already done so, create your site topology data or integrate with a Polycom RealPresence Resource Manager or CMA system to obtain it. See

2   Determine how you want to organize your sites into territories in order to best distribute responsibilities and workload among the clusters of your supercluster. A number of strategies are possible. For instance, with a five-cluster supercluster, you could adopt one of the following schemes:

   —   Create four territories, assign a primary cluster for each, and assign the fifth cluster as backup for all four.

   —   Create five territories, assign a primary cluster for each, and make each cluster the backup for one of the other territories.

   —   Use some hybrid of the above that best suits your enterprise network's distribution of sites, users, and traffic.

   Keep in mind that only three territories can host conference rooms.

   Note

   If you've integrated with a Polycom RealPresence Resource Manager or CMA system, site topology data comes from that system and can't be edited in the DMA system. You must create the territories needed in the RealPresence Resource Manager or CMA system.

3   Create the territories needed, assign functionality responsibilities to the territories, and assign primary and backup clusters to the territories.

> **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 version upgrades will not be compatible. Major version software upgrades of a supercluster take careful planning. See "Incompatible Software Version Supercluster Upgrades" on page 395.
>
> 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 24.
>
> Superclustering is not supported in **Maximum security** mode. See "The Consequences of Enabling Maximum Security Mode" on page 54.

See also:

"DMAs" on page 229

"Supercluster Procedures" on page 233

DMAs

The **DMAs** page lets you create, view, and manage a *supercluster* of Polycom DMA systems (see "About Superclustering" on page 227).

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 RealPresence Resource Manager or CMA system, join the other cluster to it, not the other way around.

Note

You can't add a Polycom RealPresence Resource Manager or CMA system to a supercluster or create a supercluster with a Polycom RealPresence Resource Manager or CMA system. But you can integrate a Polycom DMA cluster with a Polycom RealPresence Resource Manager or CMA system in order to get site topology and user-to-device association data from the latter (see "Resource Management System Integration" on page 185). You can do this either before or after creating a Polycom DMA supercluster. The site topology and user-to-device association data is replicated throughout the 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. If the cluster you're removing is responsible for any territories (as primary or backup), you must first reassign those territories. The cluster being removed may be either the one you're logged into or another cluster. The system prompts you to confirm.

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.

Warning

Restart Supercluster Services and **Reset Supercluster Services** are *emergency actions* that should only be taken when instructed to do so by a Polycom Global Services representative. They're intended only for resolving data store replication problems that can't be resolved by other means.

Restart Supercluster Services restarts supercluster services on the selected cluster. All calls are terminated and the cluster becomes unresponsive for a short period of time.

Reset Supercluster Services hard-resets supercluster services on the selected cluster and resets the cluster to its initial defaults. *This results in the loss of data.* All calls are terminated, and the cluster is forced to leave the supercluster and rebooted.

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.
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:

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 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 24.

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. We strongly recommend specifying the FQDN of the virtual management interface for the cluster to be joined.
User name	An administrator login name for the specified cluster.
Password	The password for the administrator login.

See also:

Supercluster Procedures

Note

Prior to creating a supercluster, we recommend verifying that DNS can resolve all FQDNs of all clusters to become part of the supercluster. To do so, go to **Maintenance > Troubleshooting Utilities > Ping** and ping the FQDNs (virtual and physical) of the other cluster(s). Do this on each cluster.

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. The join operation may take several minutes, and the time required increases as the number of clusters in the supercluster increases.

3 In the **Join Supercluster** dialog box, do one of the following:

— To create a new supercluster, enter the FQDN or host name of the virtual management interface for 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 FQDN or host name of the virtual management interface 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 24.

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 may be in an inconsistent state when it's brought back on line. If this occurs, the system attempts to auto-correct the situation. But if the auto-correction steps fail, 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 149.

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 227

"DMAs" on page 229

"Join Supercluster Dialog Box" on page 232

10

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

- History Retention Settings

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), and bandwidth management.

> **Note**
>
> SIP and XMPP signaling are not supported in **Maximum security** mode. See "The Consequences of Enabling Maximum Security Mode" on page 54.

The system can also function as an H.323 <-> SIP gateway.

> **Note**
>
> In H.323, DTMF tones are usually sent over the H.323 signaling path. In SIP, DTMF tones are usually sent over the media path as a special RTP payload packet (see RFC 4733). Because of this difference and because the DMA system isn't in the media path, its gateway function doesn't support DTMF transmission.
>
> The gateway function also doesn't support content sharing or AES encryption.
>
> The DMA system's gateway function is used only for calls to registered endpoints, SIP peers, and H.323 gatekeepers. It's not used for calls to virtual meeting rooms (VMRs), virtual entry queues (VEQs), external addresses, or IP addresses.

In addition, the system can be integrated with a Juniper Networks Service Resource Controller (SRC) to provide bandwidth assurance services.

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 DMAgatekeeper informed endpoint A of endpoint B's IPv4 signaling IP.

See also:

"Call Server Configuration" on page 237

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 configured site or territory can register with the Call Server. 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 Call Server accepts H.323 location requests (LRQs) only from gatekeepers configured on **External Gatekeeper** page (see "External Gatekeeper" on page 103).
Resolve H.323 Email-ID dial strings to other registered H.323 aliases	If this option is selected, the Call Server resolves email ID dial strings to another local alias by using the user part of the email address. For example, the dial string 1234@mycompany.com 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 Call Server permits rogue endpoints to place and receive calls. Rogue endpoints are endpoints in sites managed by the DMA system that are not actively registered with the system. Turning this option off blocks calls from and to rogue endpoints. Such calls are blocked even if the endpoints are registered to a neighbored gatekeeper or SIP peer. This option has no effect on other unregistered network devices (such as MCUs, GKs, and SBCs).

Table 10-1   Fields on the Call Server Settings page (continued)

Field	Description
Allow calls to inactive endpoints	If this option is selected, the Call Server considers inactive as well as active endpoints when attempting to resolve an address using the *Dial registered endpoints by alias* dial rule (see "The Default Dial Plan and Suggestions for Modifications" on page 246). Turning this option off can prevent the aliases of registrations that are no longer active from masking the aliases of endpoints registered to other call servers. This is useful in situations where an endpoint might have an active registration with one Call Server and an inactive registration with another (such as a mobile device that moves from a Call Server handling registrations through an SBC to a different Call Server in the network).
Terminate calls based upon failed responses to IRQs	If this option is selected, the Call Server terminates a call if it sends an IRQ (Information Request) to the endpoint and receives either no response or an IRR (Information Request Response) containing an invalidCall field. This is the correct behavior according to the H.323 ITU Specification, and it prevents a call license from being used unnecessarily for a call that's no longer active. Some endpoints (VVX prior to v.4.0.1, Sony PCS1, XG80, and G70, and possibly others) don't properly handle IRQ/IRR messaging, causing active calls to be disconnected if this option is selected. To avoid this problem with such endpoints, leave this option off.
Gatekeeper call mode	**Direct call mode** — 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. **Routed call mode** — The gatekeeper proxies all H.323 signaling messages.
Available bandwidth limit (percent)	Sets the maximum percentage of the available bandwidth that can be allocated to a single call. If the requested bandwidth exceeds this value, the gatekeeper "downspeeds" (reduces the bit rate of) the call, but only to the user's downspeed minimum. If there is insufficient bandwidth to comply with both this setting and the downspeed minimum, the call is rejected.
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.

Table 10-1   Fields on the Call Server Settings page (continued)

Field	Description
Registration refresh interval (seconds)	For H.323 endpoints, specifies how often registered endpoints send "keep alive" messages to the Call Server. Endpoints that fail to send "keep alive" messages on time are flagged as inactive.
	For SIP endpoints, specifies the refresh interval used if the endpoint didn't specify an interval or specified one greater than this value.
	Must be greater than or equal to the minimum SIP registration interval and in the range 150-9999.
Minimum SIP registration interval (seconds)	The minimum time between "keep alive" messages to SIP endpoints.
	Must be less than or equal to the registration refresh interval and in the range 150-3600.
IRQ sending interval (seconds)	The interval at which the system sends IRQ messages to H.323 endpoints in a call, requesting QoS (quality of service) reports.
	Must be in the range 10-600.
SIP peer timeout (seconds)	The timeout value for calls to peer proxy servers, after which the dial attempt is canceled.
	Must be in the range 3-300. To avoid call forwarding failures when a SIP peer is involved, this value must be larger than **Timeout for call forwarding when no answer**.
Territory failover delay (seconds)	The number of seconds a territory's backup cluster waits after losing contact with the primary before it takes over the territory.
	Must be in the range 6-300.
Timeout for call forwarding when no answer (seconds)	The number of seconds to wait for the called endpoint to answer (fully connect) before forwarding the call, if call forwarding on no answer is enabled for the called endpoint.
	Must be in the range 5-32.
SIP max breadth	The maximum number of concurrent parallel branches due to forking of a request.

See also:

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 250) 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.
>
> In some circumstances (depending on network topology and configuration), dialing loops can develop if you don't restrict the DMA system to specific domains.

The following table describes the fields on the page.

Table 10-2   Fields on the Domains page

Field	Description
Add new domain	Enter a domain and click **Add** to add it to the **Authorized domains** list.
	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:
	eng.mycompany.com fin.mycompany.com
	And eng.*.mycompany.com matches:
	eng.sanjose.mycompany.com eng.austin.mycompany.com
Authorized domains	The list of domains from which the system accepts registrations. Select a domain and click **Remove** to remove it from the list.
	Click **Restore Defaults** to remove all domains so that the system accepts registrations from any domain.

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.
Conference rooms belong to every local domain	Specifies that if the dial string begins with the dial-in number of a conference room (VMR) on the Polycom DMA system, a dial rule implementing the **Resolve to conference room ID** action (such as dial rule #2 of the default dial plan) ignores the domain, if any, and routes the call to that conference room. If this option is not selected, a dial string that includes a domain doesn't match a **Resolve to conference room ID** dial rule.

See also:

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 Call Server can optionally have a separate dial plan used only for untrusted ("unauthorized" or "guest") SIP calls. These are calls from devices that are not registered with the Polycom DMA system and are outside the corporate firewall (but not part of a federated enterprise). These calls typically come to the DMA system via session border controllers (SBCs) such as a Polycom RealPresence Access Director or Acme Packet Session Border Controller device.

You can configure the system to recognize and accept such calls on the **Signaling Settings** page (see "H.323 and SIP Signaling" on page 71). On the **Dial Rules** page, you can route these calls to specific VMRs (virtual meeting rooms) or VEQs (virtual entry queues), or to a specific SIP peer by creating a separate set of "guest" dial rules used only for these untrusted calls.

A dial rule consists of an optional preliminary script you can create to modify dial strings and the action to be performed, which you select from a well-defined list of actions. These actions encapsulate potentially complex dial resolution logic, which shields you from having to deal with these complexities.

For instance, the **Resolve to registered endpoint** action applies all the associated system configurations and performs various searches on the internal endpoint registration records to determine if the inbound call is attempting to reach another registered endpoint. It automatically adjusts for signaling protocol (SIP/H.323), case, and standard dial string deviations to locate a registered endpoint. You don't have to account for these variables in your dial plan because the logic behind the action does so for you.

You can test the current dial rules using the **Test Dial Rules** command. In the dialog box it opens, you can specify various caller parameters and a dial string, and see how the current dial rules handle such a call. See "Test Dial Rules Dialog Box" on page 245.

The **Dial Rules** page contains two lists, one for authorized calls and one for unauthorized calls. The former contains the system's default dial plan. The latter is empty unless you add rules to it. Both lists contain the same fields. The following table describes the fields in the two lists.

Table 10-3   Fields in the Dial Rules lists

Column	Description
Order	The priority order of the rules. Use the **Move Up** and **Move Down** commands to change the priority of a rule.
Description	Brief description of the rule.
Action	Action performed by the rule.

Table 10-3   *Fields in the Dial Rules lists (continued)*

Column	Description
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 237

"The Default Dial Plan and Suggestions for Modifications" on page 246

"Add Dial Rule Dialog Box" on page 250

"Edit Dial Rule Dialog Box" on page 252

"Test Dial Rules Dialog Box" on page 245

"Preliminary/Postliminary Scripting" on page 254

Test Dial Rules Dialog Box

The **Test Dial Rules** dialog box provides a testing mechanism for the current dial plan. You can specify various caller parameters and a dial string, and see how the each dial rule handles such a call and what its final disposition is.

The following table describes the fields in the **Test Dial Rules** dialog box.

Table 10-4   *Test Dial Rules dialog box*

Field	Description
Caller site	Select a site in order to set the four caller site variables (CALLER_SITE_NAME, CALLER_SITE_DIGITS, CALLER_SITE_COUNTRY_CODE, and CALLER_SITE_AREA_CODE). They can't be set directly and are display only.
CALLER_H323ID	Test caller's H323-ID or blank.
CALLER_E164	Test caller's E.164 alias or blank.
CALLER_TEL_URI	Test caller's SIP tel: URI or blank.
CALLER_SIP_URI	Test caller's SIP sip: URI or blank.
Dial string	Enter a dial string to test. Then click **Test**. For SIP, the dial string should always specify the schema prefix (sip or sips). For example: `sips:rbruce@10.47.7.9`

Table 10-4   *Test Dial Rules dialog box (continued)*

Field	Description
Test route output	Displays the results of applying each rule (including its preliminary, if any) to the dial string. For instance, testing the dial string example shown above against the default dial plan might result in the following: #1:SipAlias[sips:rbruce@10.47.7.9] is not registered. H323-ID[rbruce] is not registered. #2:The room [rbruce] does not exist. #3:No entry queue is found. #4:Domain [10.47.7.9] is not within our administration. #5:The call was accepted by this dial rule.
Final result	Displays the final outcome of the dial rule processing. The final outcome for the example above would be: Transformed dial string is [sips:rbruce@10.47.7.9]. The call was accepted by dial rule #5.

See also:

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 10-5   *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.
4	Dial services by prefix	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. **Note:** 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
5	Dial external networks by H.323 URL, email ID, or SIP URI	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). Examples of external addresses: H323:johnsmith@someothercompany.com sip:johnsmith@someothercompany.com
6	Dial endpoints by IP address	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). 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

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, SIP peer, or simplified dialing service that can be dialed by prefix, configure the prefix range of the new service on the appropriate page. No dial plan change is necessary, since 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.

- In some circumstances (depending on the dial plan and the network topology and configuration), dial rules using the **Resolve to external address** action (like Rule 5 of the default dial plan) or the **Resolve to IP address** action (like Rule 6) can enable dialing loops to develop, especially if servers reference each other either directly or via DNS.

  Common ways to avoid dialing loops include:

  — Use domain restrictions to ensure that the DMA system and its peers are each responsible for specific domains (see "Add External SIP Peer Dialog Box" on page 109 and "Domains" on page 242).

  — Use a preliminary script like the sample script "SUBSTITUTE DOMAIN (SIP)" (see "Sample Preliminary and Postliminary Scripts" on page 258) to change the domain of a SIP URI dial string to something that won't create a dialing loop.

  — Use a postliminary script to similarly change the domain before sending to a peer.

  — Use configuration options on the peers to prevent loops.

- 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`.

- If your enterprise includes another gatekeeper and you want to route calls to that gatekeeper without a prefix, add a dial rule using the **Resolve to external gatekeeper** action.

- If your enterprise includes a SIP peer and you want to route calls to that peer without a prefix, add a dial rule using the **Resolve to external SIP peer** action.

  If you have multiple SIP peers, a call matching the rule is routed to the first one to answer. You may want to specify the domain(s) for which each is responsible (see "Add External SIP Peer Dialog Box" on page 109).

  When routing to a SIP peer, 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.

> **Note**
>
> In a mixed H.323 and SIP environment, the Polycom DMA system acts as a seamless gateway. If an H.323 device sends it a Location Request (LRQ) and the dial plan contains a dial rule using the **Resolve to external SIP peer** action, the DMA system will respond with a Location Confirm (LCF) because it can resolve the address by routing the H.323 call through its gateway to the SIP peer(s).
>
> You can prevent H.323 calls from being routed to SIP peers by restricting which calls are routed to them in one or more of the following ways:
>
> - Assign each SIP peer an authorized domain or domains (this is a good idea in any case in order to avoid dialing loops). See "Edit External SIP Peer Dialog Box" on page 114.
> - Assign each SIP peer a prefix or prefix range. See "Edit External SIP Peer Dialog Box" on page 114.
> - Add a preliminary script to the dial rule using the **Resolve to external SIP peer** action that ensures that the rule will only match a SIP address. See "Preliminary/Postliminary Scripting" on page 254.
> - Make the dial rule using the **Resolve to external SIP peer** action the last rule and ensure that all H.323 calls will match against one of the preceding dial rules.

See also:

Add Dial Rule Dialog Box

The following table describes the fields in the **Add Dial Rule** dialog box.

Table 10-6   Add Dial Rule dialog box

Field	Description
Dial Rule	
Description	The text description displayed on the **Dial Rules** 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.
Preliminary	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. "Sample Preliminary and Postliminary Scripts" on page 258 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 **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries 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. For "unauthorized call" dial rules, only these three actions are available:

• Resolve to external SIP peer

• Resolve to conference room ID

• Resolve to virtual entry queue

Table 10-7   *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. **Note:** This action employs the H.323<->SIP gateway function if applicable.
Resolve to service prefix	Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present). **Note:** For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to alice@polycom.com must be one of the following: 　sip:123alice@polycom.com 　123alice
Resolve to external SIP peer	Checks the domain of the dial string against all of the rule's selected peers, looking for a peer proxy responsible for that domain. **Note:** This action employs the H.323<->SIP gateway function if applicable. This action may be used for "unauthorized call" dial rules.
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. **Note:** This action employs the H.323<->SIP gateway function if applicable.
Resolve to external address	Determines if the dial string is a well-formed instance of an 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. This action may be used for "unauthorized call" dial rules.
Resolve to virtual entry queue	Looks for a shared-number entry queue that matches the dial string. This action may be used for "unauthorized call" dial rules.

See also:

Edit Dial Rule Dialog Box

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

Table 10-8   Edit Dial Rule dialog box

Field	Description
Dial Rule	
Description	The text description displayed on the **Dial Rules** 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.
Preliminary	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. "Sample Preliminary and Postliminary Scripts" on page 258 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 **Debug this script** to open the Script Debugging Dialog Box for Preliminaries/Postliminaries 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. For "unauthorized call" dial rules, only these three actions are available:

• Resolve to external SIP peer

• Resolve to conference room ID

• Resolve to virtual entry queue

Table 10-9   *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. **Note:** This action employs the H.323<->SIP gateway function if applicable.
Resolve to service prefix	Looks for a service prefix that matches the beginning of the dial string (not counting the URI scheme, if present). **Note:** For a SIP peer, the dial string must either include the protocol or consist of only the prefix and user name (no @domain). For instance, if the SIP peer's prefix is 123, the dial string for a call to alice@polycom.com must be one of the following: sip:123alice@polycom.com 123alice
Resolve to external SIP peer	Checks the domain of the dial string against all of the rule's selected peers, looking for a peer proxy responsible for that domain. **Note:** This action employs the H.323<->SIP gateway function if applicable. This action may be used for "unauthorized call" dial rules.
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. **Note:** This action employs the H.323<->SIP gateway function if applicable.
Resolve to external address	Determines if the dial string is a well-formed instance of an 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. This action may be used for "unauthorized call" dial rules.
Resolve to virtual entry queue	Looks for a shared-number entry queue that matches the dial string. This action may be used for "unauthorized call" dial rules.

See also:

Preliminary/Postliminary Scripting

A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule's action is performed.

A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the DIAL_STRING variable (which is initially set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule's action (if the filter criteria aren't met) or return one of the following:

• NEXT_RULE: Skips the rule being processed and passes the dial string to the next rule.

• BLOCK: Rejects the call.

See for some examples.

The following table describes the predefined variables you can use in a preliminary or postliminary script. The script can evaluate a variable or change its value (the change isn't preserved after the script completes).

Table 10-10 *Predefined variables for preliminary and postliminary scripts*

Variable	Initial value
CALLER_E164	Array variable initially set to the set of E.164 addresses of the caller. The length of the array is 0 if the caller doesn't have an E.164 address.
CALLER_H323ID	Array variable initially set to the set of H323ID addresses of the caller. The length of the array is 0 if the caller doesn't have an H323ID address.
CALLER_IS_IPV6	"TRUE" if the caller is an IPv6 endpoint. "FALSE" otherwise.
CALLER_SIP_URI	Array variable initially set to the set of SIP URI addresses of the caller. The length of the array is 0 if the caller doesn't have a SIP URI address.
CALLER_SITE_AREA _CODE	Area code of the caller's site. Blank if the site doesn't have an area code.
CALLER_SITE_COUNTRY _CODE	Country code of the caller's site. Blank if the site doesn't have a country code.
CALLER_SITE_DIGITS	The number of subscriber number digits in the caller's site (that is, the length of a phone number at the site, excluding area code). or Blank if the site doesn't have a number of digits.

Table 10-10 *Predefined variables for preliminary and postliminary scripts (continued)*

Variable	Initial value
CALLER_SITE_NAME	The name of the caller's site.
CALLER_SITE_SITE _CODE	The site code of the caller's site.
CALLER_TEL_URI	Array variable initially set to the set of Tel URI addresses of the caller. The length of the array is 0 if the caller doesn't have a Tel URI address.
DIAL_STRING	Initially set to the dial string being evaluated. If the script modifies the DIAL_STRING value, the modified value is used as the input to the dial rule action. For SIP, when the DIAL_STRING is modified by the script, it's used as shown in Table 10-11, depending on the dial rule action:

INPUT_SIP_HEADERS	For SIP calls only, an associative array containing the SIP headers in the received SIP INVITE message.
	
	Usage example:
	
	`if(INPUT_SIP_HEADERS["Supported"].matches`
	`(/.*ms-forking.*/))`
	`{`
	`...`
	`}`

OUTPUT_SIP_HEADERS	An empty associative array. Headers that the script adds to this array replace the corresponding headers in the received SIP INVITE message. If a header added to this array isn't in the received INVITE message, it's added to the INVITE message.
	
	Usage example:
	
	`OUTPUT_SIP_HEADERS["User-Agent"] = "Someone.  Not a DMA 7000.";`
	
	`OUTPUT_SIP_HEADERS["Some-Custom-Header"] = "Whatever you want";`

The following table shows how different dial rule actions apply a preliminary script's modified dial string to the output SIP headers in a SIP call.

Table 10-11 *Effect of dial rule action on output SIP headers*

Dial Rule Action	Output SIP Headers
Resolve to registered endpoint	The To header is replaced with the modified dial string. The request URI is based on the contact address of the registered endpoint, and not replaced with the modified dial string.
Resolve to external address	The To header and the request URI are both replaced with the modified dial string.
Resolve to service prefix	For a SIP peer proxy of type *OCS*: The To header is replaced with the modified dial string. The request URI is based on the address, port, and transport type of the proxy, and not replaced with the modified dial string.
	For a SIP peer proxy of type *Other*: The To header and the request URI are both replaced with the modified dial string.
Resolve to peer proxy	For a SIP peer proxy of type *OCS*: The To header is replaced with the modified dial string. The request URI is based on the address, port, and transport type of the proxy, and not replaced with the modified dial string.
	For a SIP peer proxy of type *Other*: The To header and the request URI are both replaced with the modified dial string.
Resolve to IP address	The To header and the request URI are both replaced with the modified dial string.

See also:

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, SBC, or MCU. 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 10-12 *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. Alternatively, provide the entire SIP INVITE message. Then click **Execute Script**. **Note:** For SIP, the script should always specify the schema prefix (sip or sips). For instance: `DIAL_STRING = "sip:xxx@10.33.120.58"`
Caller site	Select a site in order to set the first four caller variables.
Caller variables	Lists variables that can be used in the script to represent caller alias values. Enter an alias value to test for that variable.
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., `println` statements).
Output SIP headers	For an external SIP peer's postliminary, displays the headers produced by the script.

See also:

Sample Preliminary and Postliminary Scripts

A preliminary is an executable script, written in the Javascript language, that defines processing actions (filtering or transformation) to be applied to a dial string before the dial rule's action is performed.

A postliminary is an executable script, written in the Javascript language, that defines dial string transformations to be applied before querying an external device (gatekeeper, SIP peer, SBC, or MCU).

Transformation scripts output some modification of the DIAL_STRING variable (which is initially set to the dial string being evaluated).

Filtering scripts may pass the dial string on to the dial rule's action (if the filter criteria aren't met) or return one of the following:

- NEXT_RULE: Skips the rule being processed and passes the dial string to the next rule.

- BLOCK: Rejects the call.

The following sample scripts address many of the scenarios for which you might need a preliminary or postliminary script. You can use them as templates or starting points for your scripts.

```
/////////////////////////////
// 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:

"Preliminary/Postliminary Scripting" on page 254

"Script Debugging Dialog Box for Preliminaries/Postliminaries" on page 257

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.

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 10-13 *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 237

"Add Hunt Group Dialog Box" on page 262

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 10-14 *Add Hunt Group dialog box*

Field	Description
General Info	
Name	Hunt group name.
Description	The text description displayed in the **Hunt Groups** 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 **Add** to add an alias. Click **Edit** or **Delete** to change or remove the selected alias.
Hunt Group Members	
Search	Search for endpoints by alias, IP address, or registration status.
Available endpoints	Lists the endpoints that match the search criteria.
Member endpoints	Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.

See also:

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 10-15 Edit Hunt Group dialog box

Field	Description
General Info	
Name	Hunt group name.
Description	The text description displayed in the **Hunt Groups** 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 **Add** to add an alias. Click **Edit** or **Delete** to change or remove the selected alias.
Hunt Group Members	
Search	Search for endpoints by alias, IP address, or registration status.
Available endpoints	Lists the endpoints that match the search criteria.
Member endpoints	Lists the endpoints to include in the hunt group. Use the arrow buttons to move endpoints from one list to the other.

See also:

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:

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:

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 domain as specified on the **Network Settings** page (or `sip.dma` if no domain is specified). See "Network Settings" on page 64. This allows 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:

- Configure specific SIP digest authentication settings for SIP devices.

- Maintain the Call Server's local inbound device authentication list. This list is used for both H.235 authentication (H.323 devices) and SIP digest authentication (SIP devices).

- Click the **Signaling settings** link to go to the Signaling Settings page, where you actually enable device authentication for H.323, SIP, or both (see "Signaling Settings" on page 71).

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 on behalf of calling devices to external SIP peers for which the appropriate device-specific credentials haven't been defined.

The Call Server intercepts and responds to authentication challenges from SIP peers on behalf of some or all devices calling though the Call Server. This feature allows authentication security between the Call Server and its peers to be completely separate from security between the endpoints and the Call Server.

When you add an external SIP peer, you can specify whether the Call Server handles challenges (401 and 407) on behalf of the source of the call or passes them on to the source of the call. You can also define authentication credentials specifically for that SIP peer. See "Add External SIP Peer Dialog Box" on page 109.

> **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 104.

The following table describes the fields on the **Device Authentication** page.

Table 10-16 *Fields on the Device Authentication page*

Field	Description
Inbound Authentication	
SIP device authentication settings	
Use default realm	This option, the default, sets the realm for the Call Server to the cluster's domain as specified on the **Network Settings** page (allowing each cluster of a supercluster to have its own realm). If no domain is specified on the **Network Settings** page, the default realm value is `sip.dma`. Clear the check box to change the string in the **Realm** field.
Realm	The realm string in an authentication challenge tells the challenged device the protection domain for which it must provide credentials. Generally, it includes the domain label of the Call Server. See RFC 2617 and RFC 3261. If you specify a realm instead of using the default, the realm you specify is used for all clusters in the supercluster.

Table 10-16 Fields on the Device Authentication page (continued)

Field	Description
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.
SIP device authentication settings **Shared Outbound Authentication**	
(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 **Realm** or **Name** field and **Search** 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 "Edit External SIP Peer Dialog Box" on page 114). If there is none with the correct realm, it looks at the entries listed here.

See also:

"Call Server Configuration" on page 237

"Add Device Authentication Dialog Box" on page 266

"Edit Device Authentication Dialog Box" on page 267

"Add Authentication Dialog Box" on page 123

"Edit Authentication Dialog Box" on page 123

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 10-17 *Add Device Authentication dialog box*

Field	Description
Device Authentication	
Name	The name that the device includes in registration and signaling requests or responses to authentication challenges. **Note:** The name and password for a device are whatever values the person who configured the device specified. They don't uniquely identify a specific device; multiple devices can have the same name and password.
Password Confirm password	The password that the device includes in registration and signaling requests or responses to authentication challenges.

See also:

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 10-18 *Edit Device Authentication dialog box*

Field	Description
Device Authentication	
Name	The name that the device includes in registration and signaling requests or responses to authentication challenges. **Note:** The name and password for a device are whatever values the person who configured the device specified. They don't uniquely identify a specific device; multiple devices can have the same name and password.
Password Confirm password	The password that the device includes in registration and signaling requests or responses to authentication challenges.

See also:

"Device Authentication" on page 264

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 91 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 239). 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 10-19 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 **Ignore IP and port changes** 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 **Debug this script** to test the script with various variables. Click **Reapply policy** 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 *Inactive* (that is, their registrations have expired) are deleted from the system after the specified number of days. Some dial rule actions, such as **Resolve to registered endpoint**, can route calls to endpoints with an inactive registration. Deleting the registration record is the only way to prevent resolution to an inactive endpoint.

See also:

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 91.

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 273 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 10-20 Predefined variables for registration policy scripts

Variable	Initial value
EP_DEFINED_IN_CMA	"TRUE" if the Polycom DMA system is integrated with a RealPresence Resource Manager or CMA system and the endpoint is defined in that system.
EP_H323_DIALEDDIGITS_ALIAS	Endpoint alias value associated with H.323 dialedDigits or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_H323_EMAIL_ID_ALIAS	Endpoint alias value associated with H.323 email-ID or blank. This is an array that can contain multiple values. Separate the values with commas.

Table 10-20 *Predefined variables for registration policy scripts (continued)*

Variable	Initial value
EP_H323_H323_ID_ALIAS	Endpoint alias value associated with H.323 H323-ID or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_H323_TRANSPORTID_ALIAS	Endpoint alias value associated with H.323 transportID or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_H323_URL_ID_ALIAS	Endpoint alias value associated with H.323 URL-ID or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_IP	Endpoint IP address. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.
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_MODEL	Endpoint model.
EP_OWNER	Endpoint owner.
EP_OWNER_DOMAIN	Endpoint owner's domain.
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_SIP_SIP_URI_ALIAS	Endpoint alias value associated with SIP sip: URI or blank. This is an array that can contain multiple values. Separate the values with commas.
EP_SIP_SIPS_URI_ALIAS	Endpoint alias value associated with SIP SIPS: URI or blank. This is an array that can contain multiple values. Separate the values with commas.

Table 10-20 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. This is an array that can contain multiple values. Separate the values with commas.
EP_VERSION	Endpoint software version number.
REG_IS_PERMANENT	"TRUE" if endpoint is already permanently registered. Blank otherwise.
REG_SITE_AREA_CODE	Area code of the site where the endpoint is attempting to register.
REG_SITE_COUNTRY_CODE	Country 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_SITE_NAME	Site where endpoint is attempting to register.
REG_SUBNET_IP_ADDRESS	IP address of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.
REG_SUBNET_MASK	IP mask of the subnet where the endpoint is attempting to register. Enter it here in normal dot or colon notation (such as 1.2.3.4 for IPv4). In the script, this is represented as an array. If the IP address is IPv4, there are 4 elements in the array. If the IP address is IPv6, there are 8 elements in the array.

See also:

"Registration Policy" on page 268

"Script Debugging Dialog Box for Registration Policy Scripts" on page 273

"Sample Registration Policy Scripts" on page 273

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 270 for a list of these). Select an **Endpoint Site** and **Subnet** to populate the site/subnet-related fields, which are read-only.

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:

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 270 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 268

"Registration Policy Scripting" on page 270

"Script Debugging Dialog Box for Registration Policy Scripts" on page 273

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 do the following:

- Add, edit, or delete any of the devices without having to navigate back to the specific page for that device type.

- Add, edit, or delete simplified ISDN gateway dialing services (see "Add Simplified ISDN Gateway Dialing Prefix Dialog Box" on page 277).

- Edit the name, vertical service code, or description of the forwarding and hunt group services and enable or disable them (see "Edit Vertical Service Code Dialog Box" on page 279).

The following table describes the fields in the list.

Table 10-21   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.
Service Status	Indicates whether the service or device is enabled or disabled.

See also:

Add Simplified ISDN Gateway Dialing Prefix Dialog Box

The **Add Simplified ISDN Gateway Dialing Prefix** dialog box lets you create a new prefix-driven simplified ISDN gateway dialing service for using external ISDN gateways.

> **Note**
>
> This feature is not related to the Polycom DMA system's built-in H.323<->SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways.
>
> This feature isn't supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix (see "Edit MCU Dialog Box" on page 142).

The following table describes the fields in the dialog box.

Table 10-22 Fields in the Add Simplified ISDN 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 ISDN 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 *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this service for resolution.
Use all ISDN gateways	Indicates whether this service applies to all available gateways or only those selected below.
Available ISDN gateways	Lists the ISDN gateways that have at least one session profile specifying an H.320 or PSTN protocol. See "Edit MCU Dialog Box" on page 142.
Selected ISDN gateways	Lists the selected ISDN gateways. The arrow buttons move gateways from one list to the other.

See also:

Edit Simplified ISDN Gateway Dialing Prefix Dialog Box

The **Edit Simplified ISDN Gateway Dialing Prefix** dialog box lets you edit a prefix-driven simplified ISDN gateway dialing service.

> **Note**
>
> This feature is not related to the Polycom DMA system's built-in H.323<->SIP gateway. Simplified ISDN gateway dialing is for routing calls to H.320 or PSTN protocol gateways.
>
> This feature isn't supported for calls from SIP endpoints, but SIP endpoints can make ISDN gateway calls by directly calling an MCU/gateway using its direct dial-in prefix (see "Edit MCU Dialog Box" on page 142).

The following table describes the fields in the dialog box.

Table 10-23 Fields in the Edit Simplified ISDN 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 ISDN 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 *Dial services by prefix* dial rule (in the default dial plan) to route calls to services, all dial strings beginning with an assigned prefix are forwarded to this service for resolution.
Use all ISDN gateways	Indicates whether this service applies to all available gateways or only those selected below.
Available ISDN gateways	Lists the gateways that have at least one session profile specifying an H.320 or PSTN protocol. See "Edit MCU Dialog Box" on page 142.
Selected ISDN gateways	Lists the selected gateways. The arrow buttons move gateways from one list to the other.

See also:

"Call Server Configuration" on page 237

"Prefix Service" on page 276

Edit Vertical Service Code Dialog Box

The **Edit Vertical Service Code** dialog box lets you edit a call forwarding or hunt group service invoked when callers dial the vertical service code (VSC) for that service followed by the alias. These services are included on the **Prefix Service** page and can't be deleted. But you can disable them or change their names, descriptions, or VSCs (shown in the **Prefix Range** column of the **Prefix Service** page). If you change the VSCs, be sure to inform all users of the change.

The following table describes the fields in the dialog box.

Table 10-24 Fields in the Edit Vertical Service Code dialog box

Column	Description
Type	The type of service. Display only.
Name	A display name for this service.
Code	The vertical service code (VSC) for this service. Must consist of an asterisk/star (*) followed by two digits.
	Registered endpoints can activate this feature by dialing the VSC followed by the alias. They can deactivate it by dialing the VSC alone.
Description	Brief description of the service.
Enabled	Clearing this check box lets you turn off the service.

See also:

"Call Server Configuration" on page 237

"Prefix Service" on page 276

Embedded DNS

In a superclustered configuration, the clusters that make up the supercluster automatically take over for each other in the event of an outage. In order to gain the full benefit of this feature, however, the endpoints that are registered to each cluster must re-register to a new cluster when the new cluster takes over.

This can be accomplished by specifying the gatekeeper or SIP proxy that each endpoint will register to as a site's domain name, rather than an IP address. Then, when there is a failover, the DNS A record for that site's domain name can be mapped to a different IP address, changing the Call Server that each endpoint is registered to.

The embedded DNS capability of the 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, your enterprise DNS must place the Polycom DMA system supercluster in charge of resolving a sub-domain. To do this, you must:

- Add NS records to your enterprise DNS so that it refers requests to resolve the site-based logical host name to these embedded DNS servers.

- Configure your enterprise DNS to forward requests for names in the site-based logical host name to any of the clusters in the supercluster.

See "Additional DNS Records for the Optional Embedded DNS Feature" on page 26.

The following table describes the fields on the **Embedded DNS** page.

Table 10-25 *Fields on the Embedded DNS page*

Field	Description
Enable embedded DNS service	Enables the embedded DNS servers.
Call server sub-domain controlled by DMA	The fully qualified domain name of the enterprise domain for which the DMA system is to provide DNS. For instance, for the base domain example.com, the sub-domain that the DMA system services might be: `callservers.example.com` This is the logical Call Server domain name for which you must create NS records in your enterprise DNS.

To enable DNS publishing

1 Be sure you've added the required NS records, one for each cluster in the supercluster, to your enterprise DNS and have configured it to forward requests for names in the logical Call Server domain to any of the clusters in the supercluster (see "Additional DNS Records for the Optional Embedded DNS Feature" on page 26).

2   Go to **Admin > Call Server > Embedded DNS**.

3   Click **Enable embedded DNS service**.

4   Enter the domain name of the enterprise domain for which the DMA system is to provide DNS and click **Update**.

5   Reconfigure your endpoints to register to the correct domain name for their site.

The correct domain name is:

```
callserver-<site name>.<logical Call Server domain name>
```

For instance, if the fully qualified domain name for the logical Call Server domain is callservers.example.com, the correct domain name for endpoints in the paris site is:

```
callserver-paris.callservers.example.com
```

> **Note**
>
> Enter all network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.

See also:

"Call Server Configuration" on page 237

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 10-26 *Fields on the History Retention Settings page*

Field	Description
Enable recording of registration history	Enables the system to retain Call Server registration records (see "Registration History Report" on page 417).
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).

Table 10-26 *Fields on the History Retention Settings page (continued)*

Field	Description
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 "Call History" on page 408).
Conference history records to retain	The number of conference records to retain on each cluster for retrieval on the Conference History page (see "Conference History" on page 410).
CDR export history records to retain	The number of records of CDR export operations to retain on each cluster (see "Export History" on page 409).
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 > Call Server > 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 237

11

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 logically describes your network and its interfaces to other networks, including the following elements:

- Site — A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device's IP address identifies the site to which it belongs.

- Network cloud — A Multiprotocol Label Switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and quality of service (QOS) information.

- Site link — A network connection between two sites or between a site and an MPLS network cloud.

- Site-to-site exclusion — A site-to-site connection that the site topology doesn't permit a voice or video call to use.

- Territory — A collection of one or more sites for which a Polycom DMA cluster is responsible. Territories serve multiple purposes in a Polycom DMA system deployment. See "Territories" on page 302.

Note

Site topology information provides a logical model representation of a network topology, not necessarily a fully accurate literal representation of a full network.

The Polycom DMA system uses site topology information for a variety of purposes, including cascading of conferences, bandwidth management, Session Border Controller selection, and cluster responsibility management in a supercluster. It can get it in one of two ways:

• If you have a Polycom RealPresence Resource Manager or CMA system, integrate the Polycom DMA system with it (see "Resource Management System Integration" on page 185) to automatically get its site topology information.

Note

Integration with a Polycom RealPresence Resource Manager or CMA system is not supported in **Maximum security** mode.

• If you don't have a Polycom RealPresence Resource Manager or 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 227), site topology data only needs to be created (or obtained from a Polycom RealPresence Resource Manager or 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 156.

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

The **Sites** page contains a list of the sites defined in the site topology.

If the system is integrated with a Polycom RealPresence Resource Manager or 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 239).

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.

> **Note**
> Enter all network/DNS-related information in all lower case to avoid possible case-sensitivity issues with various devices and ensure interoperability.

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.

Table 11-1   Information in the Sites list (continued)

Column	Description
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:** 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:

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
Site Info	
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 "Embedded DNS" on page 279.
Device Types	
MCUs	The number of MCUs in the site.
DMAs	The number of Polycom DMA systems in the site.

Table 11-2   Site Information dialog box (continued)

Field	Description
VBPs	The number of Polycom Video Border Proxy NAT/firewall traversal appliances in the site.
Endpoints	The number of registered endpoints in the site.
Subnets	A list of the subnets in the site.

See also:

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
General Info	
General Settings	
Site name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
Bandwidth Settings	
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth.
	This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls.
	Note: 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.
	When you specify both the bandwidth and bit rate limits, the dialog box shows you how many calls at that bit rate the specified bandwidth limit supports.

Table 11-3 *Add Site dialog box (continued)*

Field	Description
Territory Settings	
Territory	Assigns the site to a territory, and thus to a Polycom DMA cluster.
ISDN Number Assignment	
Assignment method	The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the Call Server and ISDN endpoints dialing in through an ISDN gateway. The assignment options are: • **No assignment**. Select this option when you don't want to define a range of E.164 aliases for the site. • **Manual assignment**. Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints. • **Automatic assignment**. Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias. After an E.164 alias is assigned to an endpoint, it's reserved for use as long as that endpoint remains registered with the Polycom DMA system. If you decide not to enable **Automatic assignment**, you can always manually add E.164 aliases to endpoints from the **Endpoints** page (see "Edit Device Dialog Box" on page 98). And endpoints will have any aliases with which they register.

Table 11-3   *Add Site dialog box (continued)*

Field	Description
Dialing method	The ISDN inward dialing method for the site:
	• **DID (Direct Inward Dial)**. Select this option if your ISDN gateway is provisioned with a range of phone numbers from the ISDN service provider, and each of these numbers will be assigned to an endpoint as an alias.
	• **Gateway Extension Dialing**. Select this option if your ISDN gateway's ISDN connection is provisioned with a single gateway phone number from the ISDN service provider, and endpoints will be assigned an extension (E.164 alias) that's internal to the company and doesn't correspond to any number that can be dialed on the PSTN.
	Endpoints can be dialed from the PSTN by dialing the ISDN gateway phone number, followed by a delimiter (usually a #) and the extension number. The gateway receives the full number from the PSTN and dials only the extension number on the IP network.
ISDN Outbound Dialing	
Override ITU dialing rules	Check this box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway.
	The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.
PBX access code	The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.
Country code	The country code for the site's location. Click the CC button to select from a list of countries.
	To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call's destination.
Area code	The city or area code for the site's location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field.
	To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call's destination.
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.

Polycom, Inc.   289

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.
ISDN Range Assignment (for DID dialing method)	
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 **Add** to add a new range of numbers. Click **Edit** or **Delete** 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.
ISDN Range Assignment (for gateway extension dialing method)	
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.
H.323 Routing	
Internet calls are not allowed	Disables H.323 calls to the internet.
Allowed via H.323-aware firewall	Allows H.323 calls to the internet through a firewall.

Table 11-3   Add Site dialog box (continued)

Field	Description
Allowed via H.323-aware SBC or ALG	Allows H.323 calls to the internet only through an H.323 session border controller (SBC) or application layer gateway (ALG).
Call signaling address (IPv4)	The call signaling address for the H.323 SBC.
Port	The call signaling port for the H.323 SBC.
SIP Routing	
Internet calls are not allowed	Disables SIP calls to the internet.
Allowed via SIP-aware firewall	Allows calls to the internet through a firewall.
Allowed via SIP-aware SBC or ALG	Allows calls to the internet only through a SIP session border controller (SBC) or application layer gateway (ALG).
Call signaling address (IPv4)	The call signaling address for the SIP SBC.
Port	The call signaling port for the SIP SBC.
Subnets	Lists the subnets in the site. Click **Add** to add a subnet. Select a subnet in the table and click **Edit** or **Delete** to modify or remove it.
Subnet Name	The unique name of the subnet.
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. **Note:** 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.

See also:

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
General Info	
General Settings	
Site name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
Bandwidth Settings	
Max bandwidth (Mbps)	The total bandwidth limit for voice and video calls. If not selected, voice and video calls can use all of the available bandwidth. This setting lets you restrict voice and video calls to only a portion of the available bandwidth, ensuring that some bandwidth always remains available for other network traffic.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls. **Note:** 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. When you specify both the bandwidth and bit rate limits, the dialog box shows you how many calls at that bit rate the specified bandwidth limit supports.
Territory Settings	
Territory	Assigns the site to a territory, and thus to a Polycom DMA cluster.

Table 11-4   *Edit Site dialog box (continued)*

Field	Description
ISDN Number Assignment	
Assignment method	The ISDN number assignment method for the devices in this site. The numbers being assigned are endpoint aliases in the form of E.164 numbers, which can be dialed by both IP endpoints registered to the Call Server and ISDN endpoints dialing in through an ISDN gateway. The assignment options are: • **No assignment**. Select this option when you don't want to define a range of E.164 aliases for the site. • **Manual assignment**. Select this option to define a range (or ranges) of E.164 aliases for the site, but not automatically assign those aliases to endpoints. • **Automatic assignment**. Select this option to define a range (or ranges) of E.164 aliases for the site and automatically assign those aliases to endpoints that register without an alias. After an E.164 alias is assigned to an endpoint, it's reserved for use as long as that endpoint remains registered with the Polycom DMA system. If you decide not to enable **Automatic assignment**, you can always manually add E.164 aliases to endpoints from the **Endpoints** page (see "Edit Device Dialog Box" on page 98). And endpoints will have any aliases with which they register.
Dialing method	The ISDN inward dialing method for the site: • **DID (Direct Inward Dial)**. Select this option if your ISDN gateway is provisioned with a range of phone numbers from the ISDN service provider, and each of these numbers will be assigned to an endpoint as an alias. • **Gateway Extension Dialing**. Select this option if your ISDN gateway's ISDN connection is provisioned with a single gateway phone number from the ISDN service provider, and endpoints will be assigned an extension (E.164 alias) that's internal to the company and doesn't correspond to any number that can be dialed on the PSTN. Endpoints can be dialed from the PSTN by dialing the ISDN gateway phone number, followed by a delimiter (usually a #) and the extension number. The gateway receives the full number from the PSTN and dials only the extension number on the IP network.

Table 11-4   *Edit Site dialog box (continued)*

Field	Description
ISDN Outbound Dialing	
Override ITU dialing rules	Check this box to override the standard dialing rules, established by the International Telecommunications Union, when dialing out using an ISDN gateway. The default setting, which does not override ITU dialing rules, is usually accurate for placing outbound calls. Enable this setting if you find that ISDN gateway calls from registered endpoints in this site are unsuccessful.
PBX access code	The code needed to access the ISDN/PSTN network through the site's PBX when dialing out.
Country code	The country code for the site's location. Click the CC button to select from a list of countries. To apply ITU dialing rules, the system must compare the country code of the gateway site with the country code of the call's destination.
Area code	The city or area code for the site's location. Leading zeroes are optional. For example, the city code for Paris is 01, but you can enter either 01 or 1 in this field. To apply ITU dialing rules, the system must compare the area code of the gateway site with the area code of the call's destination.
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.
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.
ISDN Range Assignment (for DID dialing method)	
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.

Table 11-4   Edit Site dialog box (continued)

Field	Description
ISDN Number Ranges	The number ranges available for assignment to endpoints in the site.
	Click **Add** to add a new range of numbers. Click **Edit** or **Delete** 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.
ISDN Range Assignment (for gateway extension dialing method)	
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.
H.323 Routing	
Internet calls are not allowed	Disables H.323 calls to the internet.
Allowed via H.323-aware firewall	Allows H.323 calls to the internet through a firewall.
Allowed via H.323-aware SBC or ALG	Allows H.323 calls to the internet only through an H.323 session border controller (SBC) or application layer gateway (ALG).
Call signaling address (IPv4)	The call signaling address for the H.323 SBC.
Port	The call signaling port for the H.323 SBC.
SIP Routing	
Internet calls are not allowed	Disables SIP calls to the internet.
Allowed via SIP-aware firewall	Enables calls to the internet through a firewall.
Allowed via SIP-aware SBC or ALG	Enables calls to the internet through a session border controller (SBC) or application layer gateway (ALG).

Table 11-4   *Edit Site dialog box (continued)*

Field	Description
Call signaling address (IPv4)	The call signaling address for the SBC.
Port	The call signaling port for the SBC.
Subnets	Lists the subnets in the site. Click **Add** to add a subnet. Select a subnet in the table and click **Edit** or **Delete** to modify or remove it.
Subnet Name	The unique name of the subnet.
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. **Note:** 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.

See also:

"About Site Topology" on page 283

"Sites" on page 285

"Add Subnet Dialog Box" on page 297

"Edit Subnet Dialog Box" on page 298

"Site Topology Configuration Procedures" on page 307

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
Name	The name of the subnet. Required and must be unique.
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. If not specified, the site limit applies.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls. If not specified, the site limit applies. **Note:** 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. When you specify both the bandwidth and bit rate limits, the dialog box shows you how many calls at that bit rate the specified bandwidth supports.

Note

You can assign a subnet to only one site.

See also:

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
Name	The name of the subnet. Required and must be unique.
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. If not specified, the site limit applies.
Max bit rate (kbps)	The per-call bit rate limit for voice and video calls. If not specified, the site limit applies. **Note:** 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. When you specify both the bandwidth and bit rate limits, the dialog box shows you how many calls at that bit rate the specified bandwidth supports.

Note

You can assign a subnet to only one site.

See also:

"Add Site Dialog Box" on page 287

"Edit Site Dialog Box" on page 292

"Site Topology Configuration Procedures" on page 307

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 305). Links between sites must be configured in order to enable calls between sites. In order for an endpoint in site A to call an endpoint in site B, there must be a link path (either direct, via other linked sites, or via an MPLS network cloud) connecting site A and site B.

If the system is integrated with a Polycom RealPresence Resource Manager or 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. Can't be changed when creating a site-to-cloud link.
To Site	The destination site (or MPLS cloud) of the link. Can't be changed when creating 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:

Add Site Link Dialog Box

Lets you define a new site link in the Polycom 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 305).

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.
To site	The destination site 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:

Edit Site Link Dialog Box

Lets you edit a site link in the Polycom 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 305).

You can't change the sites that a site link connects. To modify how sites are linked, delete the links to be removed and add the new links.

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 (view only).
To site	The destination site of the link (view only).
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 283

"Site Links" on page 299

"Site Topology Configuration Procedures" on page 307

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 RealPresence Resource Manager or 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 283

"Add Site-to-Site Exclusion Wizard" on page 301

"Site Topology Configuration Procedures" on page 307

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:

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, retrieving user and group data, and updating the shared supercluster data.

- Microsoft Exchange server integration (for calendaring service) is associated with a territory, thus specifying which 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 RealPresence Resource Manager or 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 RealPresence Resource Manager or 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.
Host Conference Rooms	Indicates whether this territory is used for hosting conference rooms (VMRs, or virtual meeting rooms).
Territory Summary pane	Repeats the name and description of the selected territory.
Associated Sites pane	List the sites included in the selected territory.

See also:

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
Territory Info	
Name	A meaningful name for the territory (up to 128 characters).
Description	A brief description of the territory (up to 200 characters).

Table 11-12   Add Territory dialog box (continued)

Field	Description
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 enabled for conference room hosting. No more than three territories may have this capability enabled.
Associated Sites	
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 **Associated sites** 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 **OK**.

See also:

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
Territory Info	
Name	A meaningful name for the territory (up to 128 characters).
Description	A brief description of the territory (up to 200 characters).

Table 11-13   *Edit Territory dialog box (continued)*

Field	Description
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 enabled for conference room hosting. No more than three territories may have this capability enabled.
Associated Sites	
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 **Associated sites** 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 **OK**.

See also:

Network Clouds

The **Network Clouds** page contains a list of the MPLS (Multiprotocol Label Switching) network clouds defined in the site topology.

Note

Don't confuse this with the Internet/VPN site. MPLS is a special technology typically offered via a private WAN environment, providing more reliability than the Internet. If your enterprise has an MPLS network cloud, you or your IT staff know about it.

If the system is integrated with a Polycom RealPresence Resource Manager or 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:

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
Cloud Info	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).
Associated Sites	
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 **Add Site Link** dialog box (see "Add Site Link Dialog Box" on page 299).
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 283

"Network Clouds" on page 305

"Site Topology Configuration Procedures" on page 307

Edit Network Cloud Dialog Box

Lets you edit an MPLS network cloud in the Polycom 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
Cloud Info	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).
Associated Sites	
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 **Add Site Link** dialog box (see "Add Site Link Dialog Box" on page 299).
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 283

"Network Clouds" on page 305

"Site Topology Configuration Procedures" on page 307

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 287.

    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 297.

    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 304.

    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 299.

    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 306.

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 299.

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 301.

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 RealPresence Resource Manager or CMA system, the site topology information from the Polycom RealPresence Resource Manager or CMA system will replace the information you entered.

See also:

"About Site Topology" on page 283

12

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 User Roles and Their Access Privileges" on page 11 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 an enterprise user to see enterprise reports, enterprise users, and groups).
	If you have a Polycom RealPresence Resource Manager system, assign this role to its login account. If API access for other clients is enabled, assign this role to the login account of any other API client that should have administrative rights and responsibilities.
	This role must be 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. Must be an enterprise user to view all enterprise users. Can view history reports.
	If you have a Polycom RealPresence Resource Manager system or any other API client, assign this role its users who should have provisioning rights and responsibilities.
	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 **Available Roles** or explicitly assigned.
	For purposes of API access, the system identifies a subcategory of Conferencing User, the Conference Room Owner, who can monitor and control his or her conferences.

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 342.

> **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

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 333.

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 163.

If you have a Polycom RealPresence Resource Manager that you want to integrate with the Polycom DMA system, you must create a local user account for the RealPresence Resource Manager system, which enables it to log into the DMA system's RealPresence Platform API. This account should have administrator and provisioner roles.

The RealPresence Resource Manager user owns the conference rooms (VMRs) it creates for preset dial-out conferences (called *Anytime* conferences in the RealPresence Resource Manager system).

See also:

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.

> **Caution**
>
> If you have a Polycom RealPresence Resource Manager system (or another API client) that connects to the DMA system's RealPresence Platform API, be aware that authorized users of that system (or other API client) can add local users, edit passcodes, add and edit conference rooms (VMRs), and view information about users and conference rooms. (Ordinary Conferencing Users can only access their own user information and the conference rooms they own.)
>
> In particular, the RealPresence Resource Manager system itself has a user login (see "Adding Users Overview" on page 313), and it owns the conference rooms created in its scheduling interface for preset dial-out conferences (referred to as *Anytime* conferences the RealPresence Resource Manager system).

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 (up to 500) are listed below.

> **Note**
>
> The DMA system's user database is unsorted. To avoid performance issues, if your query matches more than 4000 users, no attempt is made to sort the results on the server side before returning the first 500 matching records. The system simply returns the first 500 found in the database.
>
> In any case, there is no way to retrieve the next 500. To see all the users that match your search criteria, narrow your criteria so that no more than 500 users match.

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.

Table 12-2   *Information in the Users list (continued)*

Column	Description
Domain	The domain associated with the user. All users added manually to the system are in the LOCAL domain.
Class of Service	The class of service assigned to the user, which determines the priority of the user's calls.
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.
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 "User Roles Overview" on page 312.
Associated Endpoints	The endpoints associated with the user, if any.
Passcodes	The numeric passcodes specified for this user, if any: • Chairperson passcode — Passcode that identifies chairpersons in the user's conferences. • Conference passcode — Passcode that callers must enter to join the user's conferences. For enterprise users, passcodes (both kinds) generally come from the Active Directory. See "Adding Passcodes for Enterprise Users" on page 174. But you can specify an enterprise user's passcodes locally. See "Edit User Dialog Box" on page 320. For local users, you can add passcodes when you create or edit the users. See "Add User Dialog Box" on page 317. Whether passcodes are specified for the user or not, you can add or change them for a specific conference room of the user's. See "Edit Conference Room Dialog Box" on page 329.

See also:

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
General Info	
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 57).
User pass-through to CDR	Optional value to put in the userDataA field of call CDRs associated with this user. For instance, this might be a user ID from some external system or database.
Account disabled	If checked, user does not have conferencing privileges and can't log into the system management interface.

Table 12-3   Add User dialog box (continued)

Field	Description
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):
	• To the territory associated with the room specifically (see "Conference Rooms Dialog Box" on page 323).
	• 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 341).
	• Otherwise, the system's default territory (see "Conference Settings" on page 193).
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 193.
	Note: A class of service may also be assigned to an endpoint. See "Endpoints" on page 91.
Maximum bit rate (kbps)	If **Class of service** is selected, lets you specify the maximum bit rate for the user.
Minimum downspeed rate (kbps)	If **Class of service** is selected, lets you specify the minimum bit rate to which the user's calls can be reduced (downspeeded).
Associated Endpoints	
Associated endpoints	Lists the endpoints associated with the user. Click **Select** to open the **Select Associated Endpoints** dialog box and associate an endpoint with the user (see "Select Associated Endpoints Dialog Box" on page 322).
	Click **Delete** to delete an associated endpoint. A dialog box prompts you to confirm.
	Note: You can also manage endpoint associations on the **Endpoints** page (see "Associate User Dialog Box" on page 101). But if the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom RealPresence Resource Manager or CMA system.

Table 12-3   *Add User dialog box (continued)*

Field	Description
Associated Roles	
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 "User Roles Overview" on page 312.
Selected roles	Lists the roles selected for assignment to the user.
Conference Passcodes	
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.
	The passcode can also be set individually for each of the user's conference rooms.
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.
	The passcode can also be set individually for each of the user's conference rooms.

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:

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
General Info	
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 "Local Password" on page 57).
User pass-through to CDR	Optional value to put in the `userDataA` field of call CDRs associated with this user. For instance, this might be a user ID from some external system or database.
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.
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): • To the territory associated with the room specifically (see "Conference Rooms Dialog Box" on page 323). • 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 341). • Otherwise, the system's default territory (see "Conference Settings" on page 193).

Table 12-4   *Edit User dialog box (continued)*

Field	Description
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 193.
	Note: A class of service may also be assigned to an endpoint. See "Endpoints" on page 91.
Maximum bit rate (kbps)	If **Class of service** is selected, lets you specify the maximum bit rate for the user.
Minimum downspeed rate (kbps)	If **Class of service** is selected, lets you specify the minimum bit rate to which the user's calls can be reduced (downspeeded).
Associated Endpoints	
Associated endpoints	Lists the endpoints associated with the user. Click **Select** to open the **Select Associated Endpoints** dialog box and associate an endpoint with the user (see "Select Associated Endpoints Dialog Box" on page 322).
	Click **Delete** to delete an associated endpoint. A dialog box prompts you to confirm.
	Note: You can also manage endpoint associations on the **Endpoints** page (see "Associate User Dialog Box" on page 101). But if the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom RealPresence Resource Manager or CMA system.
Associated Roles	
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 "User Roles Overview" on page 312.
Selected roles	Lists the roles selected for assignment to the user.

Table 12-4   *Edit User dialog box (continued)*

Field	Description
Conference Passcodes	
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.
	The passcode can also be set individually for each of the user's conference rooms.
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.
	The passcode can also be set individually for each of the user's conference rooms.

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:

Select Associated Endpoints Dialog Box

Note

If the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system, it receives user-to-device association information from that system, and you can only associate users with devices on the Polycom RealPresence Resource Manager or 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 101).

See also:

Conference Rooms Dialog Box

Lets you view, add, edit, and delete the selected user's conference rooms (virtual meeting rooms, or VMRs). 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.

In addition, if you have a Polycom RealPresence Resource Manager system connected to the DMA system's RealPresence Platform API, the RealPresence Resource Manager system can create conference rooms (VMRs) in the DMA system. There are two kinds:

- Scheduled meeting conference rooms, which are short-lived (they have a start and end time). These rooms belong to the Conferencing Users who set up the meetings in the RealPresence Resource Manager system's scheduling interface.

- Preset dial-out conference rooms (called *Anytime* conferences in the RealPresence Resource Manager system), which can be used at any time by someone with the chairperson passcode to initiate a dial-out conference to a preset list of participants. These rooms belong to the user account with which the RealPresence Resource Manager logs in.

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 meeting (Polycom Conferencing for Outlook) conference rooms.
Dial-in #	Number used to dial into conference room. Automatically set to the dialing prefix (see "Conference Settings" on page 193) 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 "Conference Templates" on page 195. 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 "MCU Pool Orders" on page 156. The pool order assignment can be made at the conference room level, AD group level, or system default level.
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, user level, AD group level, or system default level.
Max Participants	Maximum number of callers allowed to join the conference. **Automatic** means the MCU's maximum is used.
Initial Start Time	For a conference room created by the Polycom DMA system for a calendared meeting (Polycom Conferencing for Outlook), the start time and date of the meeting. For a conference room created by the Polycom RealPresence Resource Manager system (via the DMA system API) for a scheduled meeting, the start time and date of the meeting.
Expiration Time	For a conference room created by the Polycom RealPresence Resource Manager (via the DMA system API) for a scheduled meeting, the end time and date of the meeting.

Table 12-5   *Conference Rooms dialog box (continued)*

Field	Description
Add	Opens the **Add Conference Room** dialog box, where you can create a new custom conference room for this user.
Edit	Opens the **Edit Conference Room** 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, calendared meeting (Polycom Conferencing for Outlook) conference rooms, or scheduled conference rooms created by the Polycom RealPresence Resource Manager system via the API. You can only delete custom conference rooms added manually in the Polycom DMA system or via the API.

See also:

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 **Generate** to let the system pick an available ID (from the range set in Conference Settings).
	If using alphanumeric conference room IDs, don't include multiple consecutive spaces or the following characters:
	()&%#@|"':;,
	If the ID includes any other punctuation characters, it must start with an alphabetic character and end with an alphanumeric character.
Dial-in #	Number used to dial into conference room. Automatically set to the dialing prefix (see "Conference Settings" on page 193) plus room ID.
Territory	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).
	If not selected, the conference room is assigned as follows (in priority order listed):
	• To the territory associated with the user (see "Edit User Dialog Box" on page 320).
	• 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 341).
	• Otherwise, the system's default territory (see "Conference Settings" on page 193).
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 "Conference Templates" on page 195.
	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 "Conference Settings" on page 193.
MCU pool order	MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. See "MCU Pool Orders" on page 156.
	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 "Conference Settings" on page 193.

Table 12-6   Add Conference Room dialog box (continued)

Field	Description
Max participants	Maximum number of callers allowed to join the conference. **Automatic** means the MCU's maximum is used.
	If not selected, the room uses the system's default maximum. See "Conference Settings" on page 193.
Chairperson passcode	The numeric passcode that identifies chairpersons in this room's conferences. If none, the room's conferences don't include the chairperson feature.
	If the user has a chairperson passcode, it appears here. You can change it to assign a different passcode for this room only.
	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 this room's conferences. If none, the room's conferences don't require a passcode.
	If the user has a conference passcode, it appears here. You can change it to assign a different passcode for this room only.
	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.
Conference room pass-through to CDR	Optional value to put in the `userDataA` field of conference CDRs associated with this user.
	For instance, this might be a user ID from some external system or database.
Conference Duration	Maximum duration of a conference (in hours and minutes) or **Unlimited** (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 "Conference Settings" on page 193.

Table 12-6   *Add Conference Room dialog box (continued)*

Field	Description
Dial-out Presets	If selected, this conference room is for a *preset dial-out* conference, referred to in the Polycom RealPresence Resource Manager system as an *Anytime* conference. When someone dials in and starts a conference, the system dials out to entries in the **Dial-out Participants** list.
	Clearing this check box lets you turn off the automatic dial-out temporarily without losing the configuration data.
	Note: To prevent unauthorized persons from being able to trigger the dial-out, be sure that you:
	• Set **Conference template** to a template that requires a chairperson to start the conference (see "Edit Conference Template Dialog Box" on page 210).
	• Specify a chairperson passcode for this conference room or this user (see "Edit User Dialog Box" on page 320).
	For further security and to prevent lines from being placed into conference without a human answering the call, specify a conference passcode as well so the called participants are prompted to enter it before being placed into conference.
	Note: The Polycom RealPresence Resource Manager system doesn't support the use of conference passcodes for Anytime conferences, only for scheduled conferences.
	Note: Dial-outs to endpoints with call forwarding set are not forwarded.
Audio-Only IVR Dial-out	Enables you to link this preset conference to an external audio conferencing bridge. Requires an RMX MCU with ISDN service configured.
	In the **Digits** field, specify the E.164 number that the RMX ISDN service must dial to connect to the audio conferencing bridge. In the **IVR DTMF** field, specify any DTMF digits (such as an access code or PIN) to send to the audio conferencing bridge after connecting (use **p** to specify a pause).
	Like the dial-outs to participants, this dial-out takes place when the conference starts.
	Note: If no RMX with ISDN service is available in the MCU pool order used by this conference room, the conference fails.
	Note: When the last participant leaves the VMR (that is, when only participants on the audio conferencing bridge remain), the link to the audio conferencing bridge is terminated and the conference ends.
Dial-out Participants	Lists the names and URIs of the participants to be automatically dialed when the conference starts.
	Click **Add** to add a participant. Click **Edit** or **Delete** to modify or remove the selected participant.

See also:

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	The unique ID of the conference room. Can't be edited for an enterprise conference room or calendared meeting (Polycom Conferencing for Outlook) conference room.
	For a custom conference room, click **Generate** to let the system pick an available ID (from the range set in Conference Settings).
	If using alphanumeric conference room IDs, don't include multiple consecutive spaces or the following characters:
	()&%#@|"':;,
	If the ID includes any other punctuation characters, it must start with an alphabetic character and end with an alphanumeric character.
Dial-in #	Number used to dial into conference room. Automatically set to the dialing prefix (see "Conference Settings" on page 193) plus room ID.
Territory	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).
	If not selected, the conference room is assigned as follows (in priority order listed):
	• To the territory associated with the user (see "Edit User Dialog Box" on page 320).
	• 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 341).
	• Otherwise, the system's default territory (see "Conference Settings" on page 193).

Table 12-7   *Edit 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 "Conference Templates" on page 195. 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 "Conference Settings" on page 193.
MCU pool order	MCU pool order used by this conference room, which is used to determine which MCU hosts a conference. See "MCU Pool Orders" on page 156. 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 "Conference Settings" on page 193.
Max participants	Maximum number of callers allowed to join the conference. **Automatic** means the MCU's maximum is used. If not selected, the room uses the system's default maximum. See "Conference Settings" on page 193.
Chairperson passcode	The numeric passcode that identifies chairpersons in this room's conferences. If none, the room's conferences don't include the chairperson feature. If the user has a chairperson passcode, it appears here. You can change it to assign a different passcode for this room only. 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 this room's conferences. If none, the room's conferences don't require a passcode. If the user has a conference passcode, it appears here. You can change it to assign a different passcode for this room only. 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.
Conference room pass-through to CDR	Optional value to put in the `userDataB` field of conference CDRs associated with this user and the userDataB field of call CDRs to this conference room. For instance, this might be a user ID from some external system or database.

Table 12-7   Edit Conference Room dialog box (continued)

Field	Description
Conference Duration	Maximum duration of a conference (in hours and minutes) or **Unlimited** (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 "Conference Settings" on page 193.
Calendar Event	This section appears only for calendared meeting (Polycom Conferencing for Outlook) conference rooms. It shows the following (read-only):
	• Start time and date (from the meeting invitation).
	• Expiration date. The conference room is deleted from the system after this date.
Dial-out Presets	If selected, this conference room is for a *preset dial-out* conference, referred to in the Polycom RealPresence Resource Manager system as an *Anytime* conference. When someone dials in and starts a conference, the system dials out to entries in the **Dial-out Participants** list.
	Clearing this check box lets you turn off the automatic dial-out temporarily without losing the configuration data.
	Note: To prevent unauthorized persons from being able to trigger the dial-out, be sure that you:
	• Set **Conference template** to a template that requires a chairperson to start the conference (see "Edit Conference Template Dialog Box" on page 210).
	• Specify a chairperson passcode for this conference room or this user (see "Edit User Dialog Box" on page 320).
	For further security and to prevent lines from being placed into conference without a human answering the call, specify a conference passcode as well so the called participants are prompted to enter it before being placed into conference.
	Note: The Polycom RealPresence Resource Manager system doesn't support the use of conference passcodes for Anytime conferences, only for scheduled conferences.
	Note: Dial-outs to endpoints with call forwarding set are not forwarded.

Table 12-7   Edit Conference Room dialog box (continued)

Field	Description
Audio-Only IVR Dial-out	Enables you to link this preset conference to an external audio conferencing bridge. Requires an RMX MCU with ISDN service configured.
	In the **Digits** field, specify the E.164 number that the RMX ISDN service must dial to connect to the audio conferencing bridge. In the **IVR DTMF** field, specify any DTMF digits (such as an access code or PIN) to send to the audio conferencing bridge after connecting (use **p** to specify a pause).
	Like the dial-outs to participants, this dial-out takes place when the conference starts.
	Note: If no RMX with ISDN service is available in the MCU pool order used by this conference room, the conference fails.
	Note: When the last participant leaves the VMR (that is, when only participants on the audio conferencing bridge remain), the link to the audio conferencing bridge is terminated and the conference ends.
Dial-out Participants	Lists the names and URIs of the participants to be automatically dialed when the conference starts.
	Click **Add** to add a participant. Click **Edit** or **Delete** to modify or remove the selected participant.

See also:

Add Dial-out Participant Dialog Box

Lets you add a participant to the conference room's **Dial-out Participants** list. When someone dials into the conference room and starts a conference, the system dials out to the participants in the list.

The following table describes the parts of the **Add Dial-out Participant** dialog box.

Table 12-8   Add Dial-out Participant dialog box

Field	Description
Participant name	The name of the participant.
Dial-out URI	Dial string used to dial the participant.

See also:

Edit Dial-out Participant Dialog Box

Lets you edit a participant in the conference room's **Dial-out Participants** list, changing the name or dial string for the participant. When someone dials into the conference room and starts a conference, the system dials out to the participants in the list.

The following table describes the parts of the **Edit Dial-out Participant** dialog box.

Table 12-9   Edit Dial-out Participant dialog box

Field	Description
Participant name	The name of the participant.
Dial-out URI	Dial string used to dial the participant.

See also:

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 334.

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 335.

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 (up to 500).

Note

The DMA system's user database is unsorted. To avoid performance issues, if your query matches more than 4000 users, no attempt is made to sort the results on the server side before returning the first 500 matching records. The system simply returns the first 500 found in the database.

In any case, there is no way to retrieve the next 500. To see all the users that match your search criteria, narrow your criteria so that no more than 500 users match.

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 317.

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 320.

    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:

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 325.

5   To set up this conference room for a *preset dial-out* conference (also known as an *Anytime* conference), select **Dial-out Presets** and do the following:

   a   Ensure that this room or user has a chairperson passcode and that you've selected a conference template that's linked to an RMX conference IVR service and requires a chairperson to start the conference.

Note

For further security and to prevent lines from being placed into conference without a human answering the call, specify a conference passcode as well so the called participants are prompted to enter it before being placed into conference.

---

   b   To link this preset conference to an external audio conferencing bridge (for hosting audio-only participants), in the **Digits** field enter the E.164 number for connecting to that bridge, and in the **IVR DTMF** field enter any DTMF digits (such as an access code or PIN) to send to the audio conferencing bridge after connecting (use **p** to specify a pause).

   This capability requires an RMX MCU with ISDN service.

   c   Under **Dial-out Participants**, add the participants to be called when the conference starts.

6   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 329.

5   To set up this conference room for a *preset dial-out conference* (also known as *anytime conference*), select **Dial-out Presets** and do the following:

   a   Ensure that this room or user has a chairperson passcode and that you've selected a conference template that's linked to an RMX

conference IVR service and requires a chairperson to start the conference.

> **Note**
>
> For further security and to prevent lines from being placed into conference without a human answering the call, specify a conference passcode as well so the called participants are prompted to enter it before being placed into conference.

b To link this preset conference to an external audio conferencing bridge, in the **Digits** field enter the E.164 number for connecting to that bridge, and in the **IVR DTMF** field enter any DTMF digits (such as an access code or PIN) to send to the audio conferencing bridge after connecting (use **p** to specify a pause).

This capability requires an RMX MCU with ISDN service.

c Under **Dial-out Participants**, add the participants to be called when the conference starts.

6 To turn of automatic dial-out temporarily without losing the configuration data, clear the **Dial-out Presets** check box.

7 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:

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 12-10 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 "Conference Settings" on page 193. **Note:** A class of service may also be assigned to a user (see "Users" on page 314) or an endpoint (see "Endpoints" on page 91).
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 "Conference Templates" on page 195. The template assignment can be made at the conference room level, AD group level, or system default level.

Table 12-10 *Fields on the Groups page (continued)*

Field	Description
MCU Pool Order	MCU pool order assigned to this group, if any, which is used to determine which MCU hosts a conference. See "MCU Pool Orders" on page 156.
	The pool order assignment can be made at the conference room level, AD group level, or system default level.
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 "User Roles Overview" on page 312.

See also:

"Users" on page 314

"Import Enterprise Groups Dialog Box" on page 339

"Edit Group Dialog Box" on page 341

"Enterprise Groups Procedures" on page 342

Import Enterprise Groups Dialog Box

The following table describes the fields in the **Import Enterprise Groups** dialog box.

Table 12-11   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 **Search**. You can use a wildcard (✳) for more complex searches, such as: • s*admins • *eng*
Search results	Lists the security groups in your Active Directory that match the search string. The system only retrieves the first 1000 groups found. If the count shows 1000, you may need to refine your search criteria.
Groups to import	Lists the groups you've selected for import, using the arrows to move them from the **Search results** box.

See also:

Edit Group Dialog Box

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

Table 12-12   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 "Conference Settings" on page 193).
Maximum bit rate (kbps)	If **Class of service** is selected, specifies the maximum bit rate for the group.
Minimum downspeed bit rate (kbps)	If **Class of service** 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 "Conference Settings" on page 193). The template assignment can be made at the conference room level, AD group level, or system default level. It defines the conference properties (or links to the RMX profile) used for its conferences. See "Conference Templates" on page 195.
MCU pool order	Select to assign the group an MCU pool order other than the system's default (see "Conference Settings" on page 193). The pool order assignment can be made at the conference room level, AD group level, or system default level. It's used to determine which MCU hosts a conference. See "MCU Pool Orders" on page 156.
Territory	Select to assign the group's conference rooms to a territory other than the system's default (see "Conference Settings" on page 193). 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, user level, AD group level, or system default level. **Note:** If a user belongs to more than one group, that user's territory setting is inherited from the lexically first group (but doesn't change if the group is renamed). To be certain that a specific user's conference rooms are assign to a specific territory, assign that territory directly to the user. See "Edit User Dialog Box" on page 320.
Conference Duration	Select to specify a maximum conference duration other than the system's default (see "Conference Settings" on page 193). If you select **Unlimited**, the maximum depends on the MCU.

Table 12-12 *Fields in the Edit Group dialog box (continued)*

Field	Description
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 "User Roles Overview" on page 312.
	Use the arrows to move roles from the **Available roles** box to the **Selected roles** box or vice versa.
Selected roles	Lists the roles you've selected for members of this group.
	Remember, ordinary Conferencing Users have no explicitly assigned role.

See also:

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 339.

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 341.

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 155 and "MCU Pool Order Procedures" on page 162.

2 Go to **User > Groups**, select the group to which you need to assign the 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 341.

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 220.

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 341.

5 Click **OK**.

See also:

"Users" on page 314

"Groups" on page 338

"Import Enterprise Groups Dialog Box" on page 339

"Edit Group Dialog Box" on page 341

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 12-13 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 server 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:

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 57). 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 12-14 *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 "Local Password" on page 57).
Confirm new password	Retype the password to confirm that you entered it correctly.

See also:

13

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 call capacity is added. See "Licenses" on page 70.

- Monitoring system health and performing the recommended regular maintenance. See "Recommended Regular Maintenance" on page 349.

- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See "Troubleshooting Utilities" on page 380. 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 388.

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 two or more DNS servers in your network configuration (see "Network Settings" on page 64). 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 69) and preferably three. Proper time management helps ensure that your cluster operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data.

- Unless otherwise instructed by Polycom Global Services, always use the **High Security** setting. See "Security Settings" on page 48.

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 81. These settings affect the number and the contents of the log archives available for download from the system. See "System Log Files" on page 377. 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 281. These settings affect how much system activity history is retained on the system and available for download as CDRs. See "Call History" on page 408, "Conference History" on page 410, and "Call Detail Records (CDRs)" on page 412.

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). Delete downloaded log archives to free up disk space.

- 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. Delete backups after downloading in order to free up disk space.

Every night, each Polycom DMA system cluster determines whether its configuration or local user data have changed. If so, it creates a configuration-only backup of the system. For details on backups, see "Backing Up and Restoring" on page 381.

General system health and capacity checks

On the **Dashboard** (see "Dashboard" on page 352), 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 **Cluster Info** pane's **Resources** section shows that there is adequate free disk space. If the system is using more than 80% of disk space, free up space by doing some or all of the following:

  — Go to **Maintenance > Backup and Restore** and download and delete backup files (see "Backing Up and Restoring" on page 381).

  — Go to **Maintenance > System Log Files** and download and delete log file archives (you must have the Auditor role to do so; see "System Log Files" on page 377).

  — Go to **Admin > Local Cluster > Logging Settings** and reducing the retention period for log archives (see "Logging Settings" on page 81).

  — Go to **Admin > Call Server > History Retention Settings** and reduce the retention values (you must have the Auditor role to do so; see "History Retention Settings" on page 281).

- 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 426) 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 418). 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 422). 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 421). Verify that the number of orphans is not unexpectedly large.

- **Reports > Enterprise Passcode Errors** (see "Enterprise Passcode Errors Report" on page 424). 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 48.

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 427.

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 412.

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. The maximum number of panes is 50.

Click the **Add Panes** button to see the panes that are available. In the **Settings** dialog box (see "Settings Dialog Box" on page 11), 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 353

"Call Server Active Calls Pane" on page 353

"Call Server Registrations Pane" on page 354

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:

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. Each "leg" of such a call is counted on the cluster it's on. The total for all clusters includes the total of all legs 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:

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 352

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 usage percentage (all cores), as reported by Hyperic SIGAR

- Memory usage (hover over the bar chart to see details)

  It's normal for memory usage to be high.

- Swap space (total and free)

- Disk space usage (actual and percentage)

- Log space usage (actual and percentage) and next scheduled log purge

Click the **Link** button to go to the **Logging Settings** page.

See also:

"Dashboard" on page 352

Conference History – Max Participants Pane

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

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

Click the **Link** button to go to the **Conference History** page.

See also:

"Dashboard" on page 352

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, IVR, and SVC), 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.

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

See also:

"Dashboard" on page 352

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 352

Exchange Server Integration Pane

If the Polycom DMA system is integrated with a Microsoft Exchange server (see "Microsoft Exchange Server Integration" on page 180), displays the following:

- The integration status, which can be one of the following:

  — **Unavailable** — A service status or inter-server communication problem prevented determination of the integration status.

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

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

  — **Primary SMTP mailbox not found** — The mailbox configured for the 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 352

License Status Pane

Displays the license status of the selected cluster and the number of licensed and active calls. Note that a call that has multiple "legs" (spans multiple clusters) uses a license for each leg of the call (each cluster it spans).

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 352

Resource Management System Integration Pane

If the Polycom DMA system is integrated with a Polycom RealPresence Resource Manager or CMA system (see "Resource Management System Integration" on page 185), displays the following:

• Host name or IP address of the RealPresence Resource Manager or CMA system.

• User name used to log into the RealPresence Resource Manager or CMA system.

• Time when site topology data was last updated from the RealPresence Resource Manager or CMA system.

• Number of territories, sites, site links, and network (MPLS) clouds in the site topology data obtained from the RealPresence Resource Manager or CMA system.

Click the **Link** button to go to the **Polycom RealPresence Resource Manager or CMA System** page.

See also:

"Dashboard" on page 352

Signaling Settings Pane

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

Click the **Link** button to go to the **Signaling Settings** page.

See also:

"Dashboard" on page 352

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:

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 operational 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 operational.

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:

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:

Alerts

On various pages and dashboard panes, the alert icon is used to indicate an abnormal condition, problem, or just 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:

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:

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 359

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 359

Alert 1101

Territory <territory> not active; Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.

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 359

Alert 1102

Territory <territory> not active; cluster <cluster> is not operational.

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:

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:

Alert 1104

Territory <territory> primary cluster <clustername> is not operational. 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-server cluster, and you can't ping either the virtual or physical IP addresses, look for a network problem. It's unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the server(s).

See also:

Alert 2001

<formatted string from server>

An error occurred when the cluster responsible for RealPresence Resource Manager or CMA integration tried to synchronized data with the Polycom RealPresence Resource Manager or CMA system. The alert text describes the nature of the problem, which may require remedial action on the Polycom RealPresence Resource Manager or CMA system.

See also:

"Alerts" on page 359

Alert 2002

Resource management server <servername> unreachable. Last contact on: YYYY-MM-DD HH:MM GMT+/-H[:MM].

The cluster responsible for RealPresence Resource Manager or CMA integration was unable to connect to the Polycom RealPresence Resource Manager or CMA system.

This may indicate a network problem or a problem with the Polycom RealPresence Resource Manager or CMA system.

Try logging into the Polycom RealPresence Resource Manager or 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 359

Alert 2004

Resource management server <servername> has inconsistent territory definitions in its site topology.

The system is integrated with a Polycom RealPresence Resource Manager or CMA system, and there is a problem with the territory definitions or responsibility assignments in the site topology data imported from that system.

On the Polycom RealPresence Resource Manager or CMA system, configure territories properly (for instance, no duplicate names) and in way that meets the needs of the DMA system. Assign responsibilities (primary and backup) for the territories to the appropriate DMA clusters. A territory can only host conference rooms if it's assigned to a DMA cluster.

See also:

"Alerts" on page 359

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 359

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 359

Alert 2103

Active Directory primary caching cluster <p-cluster> is not operational. 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-server cluster, and you can't ping either the virtual or physical IP addresses, look for a network problem. It's unlikely that both servers have failed simultaneously.

If you can ping the cluster, the OS is running, but the application may be in a bad state. Try rebooting the server(s).

See also:

Alert 2104

Active Directory service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.

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:

Alert 2105

Active Directory service is not available. Cluster <p-cluster> is not operational.

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:

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 359

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 359

Alert 2201

Calendaring primary integration cluster <p-cluster> is not operational. 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 359

Alert 2202

Calendaring service is not available. Both primary cluster <p-cluster> and backup cluster <b-cluster> are not operational.

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 359

Alert 2203

Calendaring service is not available. Cluster <p-cluster> is not operational

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 359

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 359

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 359

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 359

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 359

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:

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:

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:

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 359

Alert 3301

Cluster <cluster> is configured for 2 servers, but only a single server 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 359

Alert 3302

Cluster <cluster> is configured for 1 server, but the private interface is enabled and active.

Either the cluster contains two servers but was misconfigured as a single-server cluster, or there is only one server in the cluster but something is connected its GB2 port.

On a single-server cluster, don't use the server's GB2 port for anything.

See also:

"Alerts" on page 359

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 359

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 359

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 359

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 359

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 359

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 359

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 359

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:

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:

Alert 3601

Cluster <cluster>: System version differs between servers.

The specified cluster is supposed to have two servers, but a software version mismatch makes it impossible for them to form a redundant two-server cluster.

Possible explanations:

- Someone upgraded one server of the cluster while the other was turned off or otherwise unavailable.

- An expansion server was added to a single-server cluster, but the new server 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 359

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 359

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 359

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 359

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 359

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 359

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 359

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:

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:

Alert 4004

MCU "<MCUname>" is configured with insufficient user connections.

The system was unable to establish a management session connection to the specified MCU. This may indicate that this MCU doesn't allow sufficient connections per user.

RMX MCUs use synchronous communications. In order to efficiently manage multiple calls as quickly as possible, the Polycom DMA system uses multiple connections per MCU. By default, an RMX MCU allows up to 20 connections per user (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). We recommend not reducing this setting. If you have a DMA supercluster with three Conference Manager clusters and a busy conferencing environment, we recommend increasing this value to 30.

After a connection attempt fails and this alert is triggered, the system tries every 60 seconds to establish 5 connections to this MCU. If it succeeds, this alert is automatically cleared.

Click the link to go to the **MCUs** page.

See also:

Alert 5001

<Model> ITP system attempting to register with ID <H.323 ID> is improperly configured.

A device that identifies itself as an ITP (interactive 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:

Alert 5002

One or more endpoints is sending too much H.323 signaling traffic, has been temporarily blacklisted, and may have been quarantined.

At least one device, in violation of the H.323 standard, is sending GRQ (gatekeeper request) or RRQ (registration request) messages several times a second.

If there are many such ill-behaved devices, it could affect the DMA system's ability to provide service, so the system temporarily blacklists any such device (ignoring all signaling from it until it stops sending messages more frequently than the specification permits). If the device is or was registered, it's also quarantined, and it remains so until manually removed from quarantine.

Click the link to go to the **Endpoints** page, where you can search for endpoints with **Registration status** of **Quarantined** or **Quarantined (Inactive)**.

See also:

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:

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:

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 server'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. We recommend regularly deleting downloaded log file archives in order to free up disk space.

- **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 .

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 server.
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-server cluster, an archive is created for each server.

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:

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 device 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 347

"Recommended Regular Maintenance" on page 349

Backing Up and Restoring

Every night, each Polycom DMA system cluster determines whether its configuration or local user data have changed. If so, it creates a configuration-only backup of the system, which includes:

• Local user account information (including local data for enterprise users, such as conference room attributes)

• System configuration data

• Supercluster and resource management system integration data (if applicable)

At any time, you can create either a configuration-only backup or a full backup, which adds all the transactional data, including logs, CDRs, and audit (history) data.

The backup file is for the cluster, but on a two-server cluster, a copy of the backup exists on each server. This ensures that the backup files are available even if one of the servers isn't running.

The cluster keeps the most recent ten backups (deleting the oldest backup file when a new one is created).

Note

The system may delete backups to free up disk space if necessary.

The Polycom DMA system's **Backup and Restore** page lets you:

- Manually create a full or configuration-only backup of that cluster.

- Download backup files from the cluster for safekeeping.

- Delete backup files to free up disk space.

- Upload backup files to the cluster.

- Restore from a configuration-only backup file, returning the system state to what was backed up and leaving transactional data stores (including logs, CDRs, and audit data) empty.

- Restore from a full backup file, returning both the system state and the transactional data stores (including logs, CDRs, and audit data) to what was backed up.

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 (full or configuration-only) that you load onto the USB stick.

Note

We strongly suggest that you:

- Download backup files regularly for safekeeping

- Delete backup files after downloading in order to free up disk space.

- If you need to preserve transactional data and be able to restore it, regularly perform a full backup and download it from the cluster.

- If you have a superclustered system, download backup files from each cluster (each cluster's backup files include only the call, conference, and registration history for that cluster).

- 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 restarts the system and terminates all active conferences.

> **Note**
>
> You can restore the system while it's integrated with a Polycom RealPresence Resource Manager or 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 RealPresence Resource Manager or 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.

> **Note**
>
> You can (and should) create and download backups from clusters that are part of a supercluster, but 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.
>
> If you restore a cluster using the USB Configuration Utility while it's part of a supercluster, it's automatically removed from the supercluster.

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 (Full)** to create a full backup or **Create New (Config Only)** to create a configuration-only backup (no transaction data).

A confirmation dialog tells you the backup archive was created. For a full backup, this may take some time.

4 Click **OK**.

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 two steps of the next 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 server 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**.

9 Log back in as a local admin user and:

a In a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.

b Go to **Maintenance > Software Upgrade** and check the **Operation History** table.

    c   If the system was integrated with Active Directory, go to **Admin > Integrations > Microsoft Active Directory** and re-enable the integration.

To restore from a backup file on the cluster

1   If this is a two-server cluster, make sure that both servers 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 149.

2   If this cluster is part of a supercluster, remove it from the supercluster. See "Supercluster Procedures" on page 233.

3   Go to **Maintenance > Backup and Restore**.

4   Select the backup file from which you want to restore.

5   In the **Actions** list, click **Restore Selected**.

6   When asked to confirm that you want to restore, click **Yes**.

After a short delay, a dialog box informs you that the system is going to be restored and you'll be logged out.

7   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 server syncs to it, restoring it to the same state. Depending on the changes being applied, it may reboot so the changes can take effect.

When done, both servers' LCDs display **DMA Clustered**.

8   Log back in as a local admin user and:

    a   In a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.

    b   Go to **Maintenance > Software Upgrade** and check the **Operation History** table.

    c   If the system was integrated with AD, go to **Admin > Integrations > Microsoft Active Directory** and re-enable the integration.

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 149.

2   Shut down the system. See "Shutting Down and Restarting" on page 406.

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`.
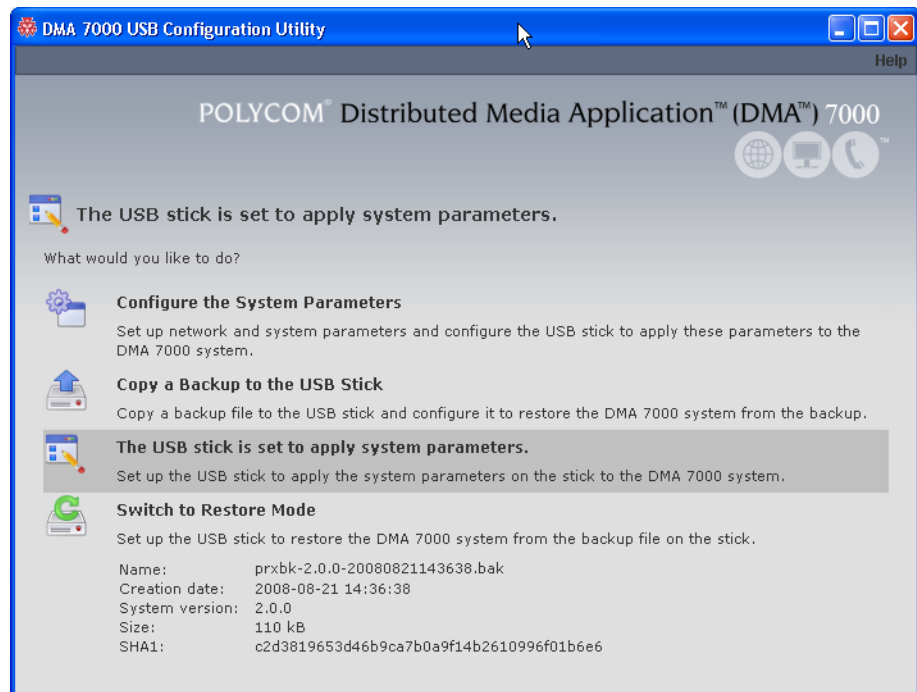
5   In the **DMA USB Configuration Utility** window, click **Copy a Backup to the USB Stick**.

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 server on (but not the other, if there are two).

If this cluster is part of a supercluster, it's automatically removed from the supercluster. 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 server has rebooted (if necessary) and its front-panel LCD displays **DMA Ready**, turn on the second server.

The second server boots, finds the first server, 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**.

11 Log back in as a local admin user and:

a   In a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.

b   Go to **Maintenance > Software Upgrade** and check the **Operation History** table.

c   If the system was integrated with Active Directory, go to **Admin > Integrations > Microsoft Active Directory** and re-enable the integration.

See also:

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.

> **Note**
>
> This version of the Polycom DMA system eliminates the need for virtual host name(s) and IP addresses in a single-server system. When a version 5.0 or earlier single-server DMA system is upgraded to version 5.1 or later, the previous version's virtual host name(s) and IP addresses become the upgraded version's physical host name(s) and IP addresses, so accessing the system doesn't change.
>
> (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server system must still have a virtual host name and IP address.)

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:

Basic Upgrade Procedures

Caution

Always check the upgrade version release notes before installing an upgrade.

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 381.

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.

The procedure below is for:

- Installing any software upgrade on a single-server or two-server system that's not part of a supercluster.

- Installing a patch (supercluster-compatible software upgrade) on a cluster that's part of a supercluster. In that case, you repeat the procedure on each cluster.

To apply a major or minor software upgrade (not supercluster-compatible) to a superclustered system, see "Incompatible Software Version Supercluster Upgrades" on page 395.

To minimize the time required for an upgrade:

- If the upgrade requires a new license, obtain the license activation key(s) ahead of time.

- Download a recent backup and upload the upgrade package file (the first five steps below) ahead of time. For a supercluster, do this on each cluster.

- Perform the remainder of the procedure during a maintenance window when there are no calls or conferences so that you can immediately take the cluster out of service instead of having to wait for all activity to end.

  Using a maintenance window with no calls on the system also eliminates any concerns about whether the remaining clusters of a supercluster have sufficient capacity to handle the load of the cluster being upgraded.

To successfully redirect certain older or third-party endpoints to a different Call Server in the supercluster, one of the following may be necessary:

- Managed endpoints may be re-provisioned by the Polycom RealPresence Resource Manager system, CMA system, or third-party endpoint management system responsible for them.

- Unmanaged endpoints may be manually reconfigured and if necessary restarted (in some cases, restarting an endpoint may be sufficient).

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 If integrated with a Polycom RealPresence Resource Manager or CMA system, go to **Admin > Integrations > Resource Management System**. and terminate the integration.

b Go to **Network > Site Topology > Territories** and reassign the cluster's territory responsibilities. Wait a few minutes and verify on another cluster that the change has been replicated.

c Go to **Network > DMAs** and take this cluster out of service (or busy it out and wait for all calls to end).

d Select this cluster and click **Remove from Supercluster**. When asked to confirm that you want to remove the cluster, click **Yes**.

The cluster is removed from the supercluster. A dialog box informs you when the process is complete. Then it logs you out and restarts.

e Click **OK** to log out immediately, or simply wait.

Note

Wait about five minutes before trying to log back into the system. You may need to restart your browser or flush your browser cache in order to log back in.

---

f Log back into the cluster you removed and verify on the **Supercluster Status** pane of the **Dashboard** that the cluster is no longer part of the supercluster.

g 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.

The **Upgrade Status** page appears. It shows progress and displays the upgrade logging. When the upgrade is complete, the system reboots.

When the upgrade and reboot are 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.

   c If the upgrade requires a new license activation key code or codes, obtain and install them as described in "Add Licenses" on page 82.

12 If this cluster is part of a supercluster, do the following:

   a Go to **Network > DMAs**, and rejoin this cluster to the supercluster. See "Supercluster Procedures" on page 233.

> **Caution**
>
> Be sure you select the cluster you just upgraded (the one you're logged into) and join it to another cluster, not the other way around.

   b Go to **Network > Site Topology > Territories** and reassign territory responsibilities back to this cluster. Or, if previously integrated with a Polycom RealPresence Resource Manager or CMA system, go to **Admin > Integrations > Resource Management System**. and reestablish the integration.

   Integration with a resource management system imports the site topology data, including territory assignments, from that system.

13 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 server for a two-server cluster.

   — The package version numbers on the two servers are not the same.

14 For a supercluster, repeat the above procedure for each additional cluster.

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 If this cluster is part of a supercluster and you're rolling back after rejoining the supercluster, do the following:

a If integrated with a Polycom RealPresence Resource Manager or CMA system, go to **Admin > Integrations > Resource Management System**. and terminate the integration.

b Go to **Network > Site Topology > Territories** and reassign the cluster's territory responsibilities. Wait a few minutes and verify on another cluster that the change has been replicated.

c Go to **Network > DMAs** and take it out of service (or busy it out and wait for all calls to end).

d Select this cluster and click **Remove from Supercluster**. When asked to confirm that you want to remove the cluster, click **Yes**.

The cluster is removed from the supercluster. A dialog box informs you when the process is complete. Then it logs you out and restarts.

e Click **OK** to log out immediately, or simply wait.

Note

Wait about five minutes before trying to log back into the system. You may need to restart your browser or flush your browser cache in order to do log back in.

f Log back into the cluster you removed and verify on the **Supercluster Status** pane of the **Dashboard** that the cluster is no longer part of the supercluster.

g Return to **Maintenance > Software Upgrade**.

4 In the **Actions** list, click **Roll Back**.

A confirmation dialog box appears.

5 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.

6 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.

7 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.

8 If this cluster is part of a supercluster, do the following:

    a Go to **Network > DMAs**, and rejoin this cluster to the supercluster. See "Supercluster Procedures" on page 233.

> **Caution**
>
> Be sure you select the cluster you just downgraded (the one you're logged into) and join it to another cluster, not the other way around.

    b Go to **Network > Site Topology > Territories** and reassign territory responsibilities back to this cluster. Or, if previously integrated with a Polycom RealPresence Resource Manager or CMA system, go to **Admin > Integrations > Resource Management System**. and reestablish the integration.

       Integration with a resource management system imports the site topology data, including territory assignments, from that system.

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 server for a two-server cluster.

    — The package version numbers on the two servers are not the same.

See also:

"Management and Maintenance Overview" on page 347

"Upgrading the Software" on page 388

Incompatible Software Version Supercluster Upgrades

All the clusters in a supercluster must be running compatible software versions. Patch releases will generally be compatible, and can be installed using the procedure in "Basic Upgrade Procedures" on page 390.

But major and minor version upgrades will not be compatible. An incompatible version software upgrade on all clusters in a supercluster requires careful 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.

You have two options for upgrading a supercluster:

- Perform the cluster upgrades in a system-wide maintenance window during which all the clusters can be shut down and the service is completely unavailable. This is by far the simplest and fastest method, taking as little as an hour or two.

- Perform the cluster upgrades incrementally so that some system capacity (although greatly reduced) remains available during the process. This method is far more complex, error-prone, and lengthy. It can easily take five or more times as long.

  During the course of an incremental 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. This requires significant configuration changes in order for some level of service to remain available, and those configuration changes must be repeated again and again as each cluster is removed from the original supercluster, upgraded, and added to the new supercluster.

  Before deciding to undertake an incremental upgrade, carefully read and consider the information in "Factors to Consider for an Incremental Supercluster Upgrade" on page 396.

Caution

We strongly recommend upgrading a supercluster only during a system-wide maintenance window when there are no calls or conferences on the system and all clusters can be taken out of service. This makes the process significantly faster and easier.

If you must upgrade incrementally, be aware of the limited capacity available at any given point in the process. It's advisable to ensure that there is little or no conferencing activity in any given territory until after the new supercluster has been created and territory responsibilities for that territory have been reassigned to a cluster in the new supercluster.

To minimize the time required for an upgrade:

- If the upgrade requires a new license, obtain the license keys ahead of time.
- Download a recent backup and upload the upgrade package file to all clusters in the supercluster ahead of time.

See also:

Factors to Consider for an Incremental Supercluster Upgrade

Before deciding to attempt an incremental supercluster software upgrade, be aware of the following:

- An incremental upgrade can easily take five times as long as the simplified method.

- As clusters are removed from the existing supercluster and upgraded, its capacity is reduced. As the new supercluster is being built, it won't be at full capacity until all clusters are upgraded. Both the existing supercluster and the new one will have limited capacity for a significant period of time, with the following possible consequences:

  - Some endpoints may be unable to register.

  - The MCUs remaining in the supercluster may not have the capacity to handle all the conferences.

  - Some endpoints may not successfully redirect their registrations and may not be able to make/receive calls.

- As the old supercluster is deconstructed, the territory associations have to be changed each time a cluster leaves. As the new supercluster is built, the territory associations have to be changed each time a cluster joins.

- As the clusters for some endpoints are removed from the existing supercluster and join the new one, the video network becomes partitioned with separate islands of endpoints.

- Some endpoints don't respond well to a gatekeeper change (such as a signaled alternate gatekeeper). To successfully redirect these endpoints to a Call Server in the new supercluster, one of the following may be necessary:

  - Managed endpoints may be re-provisioned by the Polycom RealPresence Resource Manager system, CMA system, or third-party endpoint management system responsible for them.

  - Unmanaged endpoints may be manually reconfigured and if necessary restarted (in some cases, restarting an endpoint may be sufficient).

- Any configuration changes to the old supercluster (once the first cluster has left) may be lost when the new supercluster is created.

- History records for calls and conferences that cross from the old supercluster to the new one (and vice versa) will not be merged into a single call/conference after the upgrade.

- If embedded DNS is enabled, the enterprise DNS can only point to one supercluster. The other supercluster will not have territory fail-over capability.

- If Conference Manager is enabled, during the time that the supercluster is split into two, each supercluster could host separate conferences on the same VMR.

- The site topology bandwidth specifications will be duplicated in both the old supercluster and the new supercluster. Without significant changes to the site topology's bandwidth configuration, this can lead to bandwidth overloading during the upgrade.

See also:

"Upgrading the Software" on page 388

"Basic Upgrade Procedures" on page 390

Simplified Supercluster Upgrade (Complete Service Outage)

If it's possible to schedule the upgrade for a maintenance window during which there is no service, we strongly recommend doing so, as described below. This greatly shortens and simplifies the process.

Caution

Always check the upgrade version release notes before installing an upgrade.

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 381.

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.

The procedure below is for applying a major or minor software upgrade (not supercluster-compatible) to a superclustered system.

To minimize the time required for an upgrade:

- Obtain the license activation key(s) ahead of time.

- On each cluster, download a recent backup and upload the upgrade package file (the first two steps below) ahead of time.

- Perform the remainder of the procedure during a maintenance window when there are no calls or conferences so that you can immediately take all the clusters out of service instead of having to wait for all activity to end.

To upgrade a supercluster by taking all clusters out of service

1   Put the upgrade package file somewhere on or accessible from your PC.

2   On each cluster in the supercluster, do the following:

    a   Go to **Maintenance > Software Upgrade**.

    b   In the **Actions** list, click **Upload**.

    c   Select the upgrade package file and click **Open**.

        The **File Upload** dialog box indicates when the upload is complete.

    d   Click **Close**.

        The **Upgrade Package Details** section displays information about the file you uploaded. The description includes an estimated install time.

    e   Verify that the upgrade package is correct.

3   On any cluster in the supercluster, do the following:

    a   Go to **Network > Site Topology > Territories** and record each territory's primary and backup cluster, whether it hosts conference rooms, and associated sites.

        You may need this information later to restore the configuration.

    b   If there are no active calls and conferences, skip to **d**. Otherwise, go to **Network > DMAs** and busy out each cluster in the supercluster.

        This permits existing calls and conferences to continue, but prevents new conferences and point-to-point calls from starting.

    c   On the Dashboard, monitor the **Call Server Active Calls** and **Conference Manager MCUs** panes.

    d   When all calls and conferences have ended, go to **Network > DMAs** and stop using each cluster in the supercluster.

        This completely shuts down the supercluster.

    e   Remove each cluster except the one you're logged into from the supercluster.

        As each cluster is removed, it restarts.

4   On the cluster you're logged into (let's call it cluster A), do the following:

    a   Go to **Maintenance > Software Upgrade**.

    b   In the **Actions** list, click **Upgrade**.

        A confirmation dialog box appears.

    c   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.

d Click **OK** to log out immediately, or simply wait.

The **Upgrade Status** page appears. It shows progress and displays the upgrade logging. When the upgrade is complete, the system reboots.

> **Note**
>
> If you have assistants to help you, they can perform steps 5 and 6, upgrading all the other clusters simultaneously, while the upgrade package is being installed on cluster A. If not, you can start upgrading cluster B at this point, and as soon as it restarts, start upgrading the next cluster, and so on. You don't need to wait for each cluster upgrade to be finished before starting the next one.

When the upgrade and reboot are 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.

e Log back in and, in a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.

f Go to **Maintenance > Software Upgrade** and check the **Operation History** table.

g If the upgrade requires a new license activation key code or codes, obtain and install them as described in "Add Licenses" on page 82.

5 Log into one of the other clusters (let's call it cluster B) and do the following:

a Go to **Maintenance > Software Upgrade**.

b In the **Actions** list, click **Upgrade**.

A confirmation dialog box appears.

c 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.

d 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.

    e   Log back in and, in a two-server cluster, verify on the **Dashboard** that both servers are up and the private network connection is operating properly.

    f   Go to **Maintenance > Software Upgrade** and check the **Operation History** table.

    g   If the upgrade requires a new license activation key code or codes, obtain and install them as described in "Add Licenses" on page 82.

    h   Go to **Network > DMAs** and join this cluster to cluster A to create a supercluster.

        You now have a new supercluster consisting of two upgraded clusters.

6   For each additional cluster, repeat step 5 of this procedure to upgrade it and add it to the new supercluster.

7   On any cluster of the new supercluster, do the following:

    a   Go to **Network > Site Topology > Territories** and restore the territory assignments that you recorded at step 3a of this procedure. Or, if previously integrated with a Polycom RealPresence Resource Manager or CMA system, go to **Admin > Integrations > Resource Management System**. and reestablish the integration.

        Integration with a resource management system imports the site topology data, including territory assignments, from that system.

    b   Go to **Network > DMAs** and return each cluster to service.

    c   Verify, and restore or update if necessary, other supercluster configuration settings.

    You should now have a fully functional upgraded supercluster.

8   Call Polycom Global Services if, for any cluster:

    —   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 server for a two-server cluster.

    —   The package version numbers on the two servers are not the same.

See also:

Complex Supercluster Upgrade (Some Service Maintained)

Please contact Polycom Global Services for instructions and assistance.

See also:

"Upgrading the Software" on page 388

"Basic Upgrade Procedures" on page 390

"Factors to Consider for an Incremental Supercluster Upgrade" on page 396

"Simplified Supercluster Upgrade (Complete Service Outage)" on page 397

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 5.

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 403.

• 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 404.

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 347

"Recommended Regular Maintenance" on page 349

"Expanding an Unpatched System" on page 403

"Expanding a Patched System" on page 404

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**, change **System server configuration** to **2 server configuration**, and add the Server 2 host name(s) and IP address(es) for the second server. See "Network Settings" on page 64.

   The first server (Server 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 Server 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 82.

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:

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**, change **System server configuration** to **2 server configuration**, and add the Server 2 host name and IP address for the second server. See "Network Settings" on page 64.

    The first server (Server 1) reboots.

5   Shut down the first server (Server 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 388.

8   Shut down the new server. See "Shutting Down and Restarting" on page 406.

9   Use one of the provided crossover cables to connect the GB 2 ports of the two servers.

10 Turn on the first server (Server 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 Server 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 82.

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 347

"Adding a Second Server" on page 402

"Expanding an Unpatched System" on page 403

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 403, 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 404, skipping steps 3 and 4.

See also:

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.

> **Caution**
> Don't turn off a Polycom DMA system server by simply unplugging it or otherwise removing power, especially if it's going to remain off for some time. If a server loses power without being properly shut down, the RAID controller fails to shut down, eventually depleting its battery. If that happens, the server can't be restarted without user input, requiring a keyboard and monitor.

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:

14

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 system retains the most recent 500 alerts.

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:

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**.
>
> If a call traversed multiple clusters in a supercluster, each cluster contains some of its call history data. If one of those clusters is unavailable when you view the call's history, that history may be incomplete.

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 **Export CDR Data** command (in the **Actions** list) lets you download call detail records (CDRs) for the time period you specify. See "Call Detail Records (CDRs)" on page 412.

The **Export Search Results** command lets you download just the records displayed on the page (the current search results). A **Save** dialog box prompts you to select a location for the downloaded file. The default filename is CDRSearchExport.tar. This is a troubleshooting feature. To aid in resolving a problem, Polycom Global Services may ask you to use specific search criteria to retrieve certain call records, download them, and send the file to them for analysis of the records.

The **Show Call Details** command opens the **Call Details** dialog box, which provides detailed information about the selected call. See "Call Details Dialog Box" on page 89

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
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, when available.
Destination	Destination of the call (the device's display name, if available; otherwise, its name, alias, or IP address, in that order of preference).
Start Time	Time the call began (first signaling event).
End Time	Time the call ended (session closed).
Ingress Cluster	The cluster (first, if more than one) that handled the call.
Call ID	Unique identifier for the call.

Export History

The **Call History** page's **Export History** list provides a record of the CDR exports (all call and conference data for the specified period) and search results exports from the system. It appears when you click the **Show Export History** command (in the **Actions** list).

Note

The **Export History** list is the same on the **Call History** and **Conference History** pages. In both places, all export operations are shown.

The following table describes the fields in the list. Hover over a field to see a tooltip showing the time span included in the export.

Table 14-2   Information in the Call History page Export History list

Column	Description
User	User ID of the person who performed the export.
Export Type	One of the following: • **CDR** for CDR exports • **Call History** for search results exports
Date of Export	Date and time of the export.
Cluster	The cluster from which the export took place.

See also:

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 Room ID	The conference room ID.
Start Time	Time the conference began (first conference event).
End Time	Time the conference ended (last conference event).
Cluster	The cluster that handled the conference.

Export History

The **Conference History** page's **Export History** list provides a record of the CDR exports (all call and conference data for the specified period) and search results exports from the system. It appears when you click the **Show Export History** command (in the **Actions** list).

Note

The **Export History** list is the same on the **Call History** and **Conference History** pages. In both places, all export operations are shown.

The following table describes the fields in the list. Hover over a field to see a tooltip showing the time span included in the export.

Table 14-4   *Information in the Conference History page Export History list*

Column	Description
User	User ID of the person who performed the export.
Export Type	One of the following: • **CDR** for CDR exports • **Call History** for search results exports
Date of Export	Date and time of the export.
Cluster	The cluster from which the export took place.

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 408.

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:

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"`).

The time fields contain the server times, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for `endTime` will be different from the offset for `startTime`.

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: • PT-PT • VMR • VEQ • VSC-hunt group • VSC-[uncond fwd | fwd busy | fwd no answer]
callUuid	Call UUID MSB and call UUID LSB.
startTime	YYYY-MM-DDTHH:MM:SS[+|-]HH:MM If multiple call records, the start of this segment of the call.

Table 14-7   Call CDR (continued)

Field	Description
endTime	YYYY-MM-DDTHH:MM:SS[+|-]HH: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: • h323 • sip
destSignalType	One of the following: • h323 • sip
refConfUUID	If VMR call, conf uuid appearing in Conference CDR.
lastForwardEndpoint	If call forwarding, endpoint that forwarded call to the final destination endpoint.
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: • originator • destination • callserver
bitRate	Bit rate for call, in kbps.
classOfService	Class of service for the call: • Gold • Silver • Bronze
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.

414   Polycom, Inc.

Table 14-7   Call CDR (continued)

Field	Description
VMRCluster	Virtual cluster ID; the cluster handling the VMR, or blank if not VMR call.
VEQCluster	Virtual cluster ID; the cluster handling the VEQ, or blank if no VEQ.
userDataA	The value from the **User pass-through to CDR** field of the user associated with the endpoint (see "Edit User Dialog Box" on page 320). For point-to-point calls, this is the user associated with the endpoint that started this call.
userDataB	For VMR calls, the value from the **Conference room pass-through to CDR** field of the conference room (VMR) to which the call connected (see "Edit Conference Room Dialog Box" on page 329). For point-to-point calls, the value from the **User pass-through to CDR** field of the user associated with the endpoint that received this call.
userDataC	For VMR calls, the dial-out participant pass-through value provided via the API, if any. For point-to-point calls, not currently used.
userDataD	Not currently used.
userDataE	Not currently used.
userRole	If VMR call, the role of the caller in conference (participant or chairperson). Null if not VMR call.
dialin	If this is point-to-point or a VMR dial-in call, TRUE. Otherwise, FALSE.

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.

The time fields contain the server times, with the GMT offset shown at the end. Note that if a conference spans a daylight savings time change, the offset for endTime will be different from the offset for startTime.

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: • AD-HOC • PCO (for calendared)
cluster	Virtual cluster ID; the cluster serving the VMR.
confUUID	Unique identifier for the conference.
startTime	YYYY-MM-DDTHH:MM:SS[+|-]HH:MM
endTime	YYYY-MM-DDTHH:MM:SS[+|-]HH: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: • Gold • Silver • Bronze
userDataA	The value from the **User pass-through to CDR** field of the user associated with the conference room (VMR) (see "Edit User Dialog Box" on page 320).
userDataB	The value from the **Conference room pass-through to CDR** field of the conference room (VMR) (see "Edit Conference Room Dialog Box" on page 329).
userDataC	The conference ID provided via the API, if any.

See also:

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 Detail**s 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 268).

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: • Active • Rejected • Terminated by call server • Terminated by endpoint • Timed out

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:

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	**OK** 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 **All Domains** list below.
Forest root DN	Shows the distinguished name of the Active Directory forest root domain.
Site	The Active Directory site name for the system. Available only if **Auto-discover from FQDN** (serverless bind) is selected on the Microsoft Active Directory Integration page.
	If serverless bind is enabled, but no site is retrieved, the reason could be:
	• **Site could not be determined**: the system's subnet isn't mapped to a site (see http://support.microsoft.com//kb/889031).
	• **Auto-discover failed or is disabled**: could be problem with DNS domain name or missing SRV records on DNS server.
All Domains	
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	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: • **Not required**: no groups from that domain have been imported into the Polycom DMA system and all attributes needed were in the global catalog. • **Partially loaded** or **Unable to load**: see **Error Message** and the list of groups with incomplete information for more details. 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 **Active Directory Integration** page and try again. If the system repeatedly fails to contact a domain, troubleshoot your network.
Groups with Partially Loaded or No Membership Information	
Group Name	Name of a global group whose member information is incomplete. This includes groups that directly or indirectly contain groups whose member information is incomplete. Groups with members in multiple domains that couldn't be contacted are listed for each.
Domain	Domain to which the group belongs.
Description	Description of the group.

See also:

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
Orphaned Groups	
Group ID	ID of the user group.
Domain	Domain to which the user group belonged.
Orphaned Users	
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 163

"Active Directory Integration Report" on page 418

"Enterprise Passcode Errors Report" on page 424

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 163.

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:

• Total number of users found

• 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 users with 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 users with invalid conference room IDs

- Number of users with 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 (*Blank*, *Duplicate*, or *Invalid*).
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 "Microsoft Active Directory Integration" on page 163). The column heading is the name of the attribute, such as **telephoneNumber**.
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 163

"Active Directory Integration Report" on page 418

"Orphaned Groups and Users Report" on page 421

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 174.

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.
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 163

"Adding Passcodes for Enterprise Users" on page 174

"Active Directory Integration Report" on page 418

"Orphaned Groups and Users Report" on page 421

"Conference Room Errors Report" on page 422

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
name	Name of the throttlepoint, territory, or cluster that defines the scope being measured.
date	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.
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_percent	The (maximum) percentage of the bandwidth limit used for the scope during the time interval (kbps).
packet_loss_percent	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).

Table 14-14 *Network Usage record layout (continued)*

Field	Description
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.
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.

Field	Description
h323_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_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 407

"Call History" on page 408

"About Site Topology" on page 283

15

Polycom DMA System SNMP Support

This chapter provides a discussion of the Polycom® Distributed Media Application™ (DMA™) SNMP support. It includes these topics:

- SNMP Overview
- SNMP Settings
- SNMP Procedures
- The Polycom DMA System MIB

SNMP Overview

Simple Network Management Protocol (SNMP) is a communication protocol that allows network management systems to manage resources across a network. SNMP can be transmitted over TCP or UDP.

SNMP communication takes place between the management system and SNMP agents, which are the hardware and software that the management system monitors. An agent collects and stores local system information and makes this information available to the management system via SNMP.

The Polycom DMA system software includes an SNMP agent. It translates local system information into the format defined by the Management Information Base (MIB). SNMP access to the DMA system is read-only. SET operations are not supported, but GET, GETNEXT, GETBULK, NOTIFY, and INFORM are.

The DMA system resides on a Polycom-branded Dell server running the CentOS Linux operating system. The DMA software, CentOS, and the Dell server each have their own MIB and SNMP agent. But the default Linux SNMP daemon agent (`snmpd`) aggregates the information from all three and makes it available to network management systems.

We recommend using a MIB browser to explore the PolycomDMA system MIB, but a copy of the MIB is available in "The Polycom DMA System MIB" on page 442. The DMA system MIB is self-documenting, including information about the purpose of specific traps and inform notifications.

Note that you should understand how your SNMP management system is configured in order to properly configure the DMA system's SNMP transport protocol, version, authentication, and privacy settings.

See also:

"List of Available SNMP MIBs" on page 433

"SNMP Settings" on page 433

"SNMP Procedures" on page 441

"The Polycom DMA System MIB" on page 442

SNMP Versions Supported

The Polycom DMA system supports:

• **SNMPv2c**—The Polycom DMA system implements a sub-version of SNMPv2. The key advantage of SNMPv2c is the Inform command. Unlike Traps, Informs are messages sent to the management system that must be positively acknowledged with a response message. If the management system doesn't reply to an Inform, the DMA system re-sends the Inform. SNMPv2c also has improved error handling.

One drawback of SNMPv2c is that it doesn't encrypt communications between the management system and SNMP agents, so it's subject to packet sniffing of the clear text community string from the network traffic.

• **SNMPv3**—The Polycom DMA system implements the newest version of SNMP. Its primary feature is enhanced security. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity. The `contextEngineID` is used to generate the key for authenticated messages.

The Polycom DMA system implements SNMPv3 communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB).

To implement this security level, you must define SNMP users to be added to the SNMP agent user list. Agents use this list to protect SNMPv3 packets from interception. Each user has a secret key to ensure authentication and privacy.

— Authentication ensures that only the intended recipient receives the SNMP message. As messages are created, they're given a special key that's based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.

— Privacy encrypts the SNMP message to ensure that unauthorized users can't read it.

List of Available SNMP MIBs

The following table describes the MIBs that are on the Polycom DMA system. You can download any of them from the SNMP Settings page. See "SNMP Procedures" on page 441.

Table 15-1   SNMP MIBs on the system

Name	Description
JVM-MANAGEMENT-MIB	MIB for monitoring the state of the Java Virtual Machine.
MIB-Dell-10892	The primary MIB for the Polycom-branded Dell server. It provides 36 traps from the server motherboard, including system type, voltages, and temperature readings. For more information, see the Dell SNMP documentation.
POLYCOM-BASE-MIB	Base MIB for Polycom products.
POLYCOM-DMA-MIB	DMA-specific MIB definition. See "The Polycom DMA System MIB" on page 442.
RFC1213-MIB	RFC1213 MIB definitions included for reference. The DMA system supports all but egp.
SNMPv2-CONF	A definition file for standard conventions included for reference.
SNMPv2-SMI	A definition file for standard conventions included for reference.
SNMPv2-TC	A definition file for standard conventions included for reference.

SNMP Settings

On the **SNMP Settings** page, you can:

•   Enable and configure SNMP monitoring

•   Check SNMP status

•   Maintain the notification user and agent lists

•   Download MIBs

The following table describes the fields on the page.

Table 15-2 *Information on the SNMP Settings page*

Setting	Description
Enable SNMP monitoring	Enables the SNMP settings fields below.
SNMP version	Select the version to enable: • v2c • v3 See "SNMP Versions Supported" on page 432 for a comparison of the two versions.
Transport	Specify the transport protocol for SNMP communications: **TCP**—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers support SNMP only over TCP. **UDP**—This protocol doesn't provide error-recovery services, message delivery isn't assured, and messages may not be delivered in the order sent. Because UDP doesn't have error recovery services, it requires fewer network resources. It's well-suited for repetitive, low-priority functions like alarm monitoring and is frequently used for SNMP communications.
Port	Specify the port that the Polycom DMA system uses for general SNMP messages. By default, the DMA system uses port 161.
Community	Specify the community name, which is the name of the SNMP group to which the devices and management stations running SNMP belong. The DMA system's SNMP agent is a member of only one community. By default, its name is `public`, but you should change that for security reasons. The community name is essentially a password. The DMA system will not respond to requests from management systems that don't belong to the same community. By itself, this provides only a minimal level of security; since SNMPv2c doesn't encrypt communications, the community name is sent in clear text. SNMPv3 provides much greater security. See "SNMP Versions Supported" on page 432 and the v3-specific fields below.
Contact	The name or email address of a contact person for the system. Required, but you can enter anything.
Location	The location of the system. Required, but you can enter anything.

Table 15-2   Information on the SNMP Settings page (continued)

Setting	Description
Local engine ID	When SNMP monitoring is enabled, displays the administratively unique identifier for the default context of the system's SNMP protocol engine. For SNMPv3, the local engine ID is used in generating the authentication and encryption keys.
Security user	For SNMPv3, specify the user name of the read-only SNMP access user (that is, the security user authorized to actively retrieve SNMP data).
Authentication type	For SNMPv3, specify the authentication protocol. These protocols are used to create unique fixed-size message digests of a variable length message. Possible values for authentication protocol are: • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.
Authentication password Confirm password	For SNMPv3, specify the authentication password that's used (along with the local engine ID) to create the authentication key used by the MD5 or SHA message digest.
Encryption type	For SNMPv3, specify the privacy protocol for the connection between the management system and the SNMP agent: • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption password Confirm password	For SNMPv3, specify the password that's used (along with the local engine ID) to create the encryption key used by the privacy protocol.
Notification Users (USM)	Lists the notification users that have been created. For SNMPv3, these are security users authorized to receive notifications (Traps or Informs), but not to actively retrieve SNMP data. Notification agents can send notifications to users in this list.
Notification Agents	Lists the notification agents that have been created. The system supports up to eight notification agents. The icon to the left of each entry indicates whether that agent is enabled.
Address	The IP address, port number, and transport protocol used for this agent.

Table 15-2   *Information on the SNMP Settings page (continued)*

Setting	Description
Type	The notification type for this agent: • Inform—An unsolicited message sent to a notification receiver for which the agent expects/requires a confirmation message. Introduced with SNMP version 2c, this option is not supported by systems that only support SNMP version 1. • Trap—An unsolicited message sent to a notification receiver for which the agent does not expect/require a confirmation message.
Version	The SNMP version for this agent (v2c or v3). See "SNMP Versions Supported" on page 432.
Security User	The security user to receive notifications from this agent, selected from the **Notification Users** list. For SNMPv3, a security user is required.
Minimum recurring notification interval	Select the minimum time between recurring notifications that haven't been cleared.

Add Notification User Dialog Box

The **Add Notification User** dialog box lets you add a security user authorized to receive notifications. For SNMPv3 notifications, a security user is required. When you add a notification agent, you select a security user from the list of notification users that have been added.

Notification users aren't needed or used for SNMPv2c.

The following table describes the fields in the dialog box.

Table 15-3   *Add Notification User dialog box*

Setting	Description
Security user	The security user name authorized to receive notifications (Traps or Informs).
Authentication type	The authentication protocol. These protocols are used to create unique fixed-size message digests of a variable length message. Possible values for authentication protocol are: • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.
Authentication password Confirm password	The authentication password that's used (along with the local engine ID) to create the authentication key used by the MD5 or SHA message digest.
Encryption type	The privacy protocol for the connection between the DMA system and the SNMP agent: • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption password Confirm password	The password that's used (along with the local engine ID) to create the encryption key used by the privacy protocol.

See also:

"SNMP Settings" on page 433

"Add Notification Agent Dialog Box" on page 439

"Edit Notification Agent Dialog Box" on page 440

"SNMP Procedures" on page 441

Edit Notification User Dialog Box

The **Edit Notification User** dialog box lets you modify a security user authorized to receive SNMPv3 notifications.

The following table describes the fields in the dialog box.

Table 15-4   Edit Notification User dialog box

Setting	Description
Security user	The security user name authorized to receive notifications (Traps or Informs).
Authentication type	The authentication protocol. These protocols are used to create unique fixed-size message digests of a variable length message. Possible values for authentication protocol are: • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.
Authentication password Confirm password	The authentication password that's used (along with the local engine ID) to create the authentication key used by the MD5 or SHA message digest.
Encryption type	The privacy protocol for the connection between the DMA system and the SNMP agent: • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption password Confirm password	The password that's used (along with the local engine ID) to create the encryption key used by the privacy protocol.

See also:

Add Notification Agent Dialog Box

The **Add Notification Agent** dialog box lets you add an SNMP agent to the system, specifying what kinds of notifications it sends and to whom. To limit the effect on system performance, a maximum of 8 agents may be defined.

The following table describes the fields in the dialog box.

Table 15-5   Add Notification Agent dialog box

Setting	Description
Enable agent	Enables the notification agent defined below. Clearing this check box lets you stop using this agent without deleting it.
Transport	The transport protocol for SNMP communications to the host receiver (TCP or UDP). See "SNMP Overview" on page 431.
Address	The IP address of the host receiver (the SNMP manager to whom this agent sends notifications).
Port	Specify the port that the DMA system will use to send notifications. By default, the DMA system uses port 162.
Notification type	The type of notification that this agent sends to the notification receiver: • Inform — The agent sends an unsolicited message to a notification receiver and expects/requires the receiver to respond with a confirmation message. Introduced with SNMP version 2c, this option is not supported by network management systems that only support SNMP version 1. • Trap—The agent sends an unsolicited message to a notification receiver and does not expect/require a confirmation message.
SNMP version	The version of SNMP supported (v2c or v3). See "SNMP Versions Supported" on page 432.
Security user	For SNMPv3, the security user to receive notifications from this agent. The list contains the names of the security users in the **Notification Users** list.

See also:

Edit Notification Agent Dialog Box

The **Edit Notification Agent** dialog box lets you enable, disable, or modify an SNMP notification agent.

The following table describes the fields in the dialog box.

Table 15-6   Edit Notification Agent dialog box

Setting	Description
Enable agent	Enables the notification agent defined below. Clearing this check box lets you stop using this agent without deleting it.
Transport	The transport protocol for SNMP communications to the host receiver (TCP or UDP). See "SNMP Overview" on page 431.
Address	The IP address of the host receiver (the SNMP manager to whom this agent sends notifications).
Port	Specify the port that the DMA system will use to send notifications. By default, the DMA system uses port 162.
Notification type	The type of notification that this agent sends to the notification receiver: • Inform — The agent sends an unsolicited message to a notification receiver and expects/requires the receiver to respond with a confirmation message. Introduced with SNMP version 2c, this option is not supported by network management systems that only support SNMP version 1. • Trap—The agent sends an unsolicited message to a notification receiver and does not expect/require a confirmation message.
SNMP version	The version of SNMP supported (v2c or v3). See "SNMP Versions Supported" on page 432.
Security user	For SNMPv3, the security user to receive notifications from this agent. The list contains the names of the security users in the **Notification Users** list.

See also:

"SNMP Settings" on page 433

"Add Notification User Dialog Box" on page 436

"Edit Notification User Dialog Box" on page 438

"SNMP Procedures" on page 441

SNMP Procedures

To enable and configure SNMP monitoring

1   Go to **Admin > Local Cluster > SNMP Settings**.

2   Select **Enable SNMP monitoring** and select an **SNMP version**. For information on the SNMP versions, see "SNMP Overview" on page 431.

3   Configure the SNMP version, transport protocol, and other settings. If using SNMPv3, configure the security user, authentication, and privacy settings. For descriptions, see "SNMP Settings" on page 433.

4   To enable notifications (Traps or Informs) to specified users/hosts, do the following:

   a   If using SNMPv3, add one or more notification users (see below).

   b   Add one or more notification agents (see below).

5   Click **Update**.

To add an SNMP notification user to a DMA system

1   Go to **Admin > Local Cluster > SNMP Settings**.

2   In the **Notification Users** section, click **Add User**.

3   Configure the settings in the **Add Notification User** dialog box. For descriptions, see "Add Notification User Dialog Box" on page 436.

4   Click **OK**.

The user appears in the **Notification Users** list.

To add an SNMP notification agent to a DMA system

1   Go to **Admin > Local Cluster > SNMP Settings**.

2   In the **Notification Agents** section, click **Add Agent**.

3   In the **Add Notification Agent** dialog box, select **Enable agent** and configure the settings for this agent. For descriptions, see "Add Notification Agent Dialog Box" on page 439.

4   Click **OK**.

The agent appears in the **Notification Agents** list.

To download the MIB package for a DMA system

1   Go to **Admin > SNMP Settings**.

2   Click **Download MIBs**.

3 In the **MIBs** dialog box, select the MIB of interest and click **Download**.

4 Specify a name and location, and click **Save**.

Polycom recommends using a MIB browser to explore the DMA system MIB, but a copy of the MIB is available in "The Polycom DMA System MIB" on page 442.

The DMA system MIB is self-documenting, including information about the purpose of specific traps and inform notifications.

See also:

The Polycom DMA System MIB

The `POLYCOM-DMA-MIB.mib` file is reproduced in full below. Note that a few lines are too long to fit within the page margins of this document and wrap.

```
POLYCOM-DMA-MIB DEFINITIONS ::= BEGIN


-- OUTLINE
--
-- The objects defined within this MIB are for the monitoring of the Polycom DMA 7000 system. In
the
-- table below, the object identifier has an implied base of the DMA OID:
--    iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).polycom(13885).dma(13)
--
-- OID                ENTRY
-- ===                =====
-- .1                 dmaInternal1
-- .2                 dmaMonitoring1
-- .2.1               dmaConfig
-- .2.1.1             cfgIdentity
-- .2.1.1.1           cfgProductInfo
-- .2.1.1.1.1         cfgProdInfoManufacturer
-- .2.1.1.1.2         cfgProdInfoModel
-- .2.1.1.1.3         cfgProdInfoHardwareInfo
-- .2.1.1.1.3.1       cfgProdInfoHWModel
-- .2.1.1.1.3.2       cfgProdInfoHWSerialNumber
-- .2.1.1.1.4         cfgProdInfoSoftwareInfo
-- .2.1.1.1.4.1       cfgProdInfoSWVersion
-- .2.1.1.1.4.2       cfgProdInfoSWExtendedVersion
-- .2.1.1.1.4.2.1     cfgProdInfoSWExtVerPlatformVersion
-- .2.1.1.1.4.2.2     cfgProdInfoSWExtVerApplicationVersion
-- .2.1.2             cfgServer
-- .2.1.2.1           cfgNetwork
```

```
-- .2.1.2.1.1            cfgNetworkHostname
-- .2.1.2.1.2            cfgInterfacesCount
-- .2.1.2.1.3            cfgInterfacesTable
-- .2.1.2.1.3.1          cfgInterfacesEntry
-- .2.1.2.1.3.1.1        cfgIfIndex
-- .2.1.2.1.3.1.2        cfgIfName
-- .2.1.2.1.3.1.3        cfgIfEnabled
-- .2.1.2.1.3.1.4        cfgIfMACAddress
-- .2.1.2.1.3.1.5        cfgIfIPv4Address
-- .2.1.2.1.3.1.6        cfgIfIPv4SubnetMask
-- .2.1.2.1.3.1.7        cfgIfIPv4Gateway
-- .2.1.2.1.3.1.8        cfgIfIPv6Address
-- .2.1.2.1.3.1.9        cfgIfIPv6PrefixLength
-- .2.1.3                cfgCallserver
-- .2.1.3.1              cfgCsSupercluster
-- .2.1.3.1.1            cfgCsSiteTopology
-- .2.1.3.1.1.1          cfgCsTerritoriesCount
-- .2.1.3.1.1.2          cfgCsTerritoriesTable
-- .2.1.3.1.1.2.1        cfgCsTerritoriesEntry
-- .2.1.3.1.1.2.1.1      cfgCsTerritoryIndex
-- .2.1.3.1.1.2.1.2      cfgCsTerritoryName
-- .2.1.3.1.1.2.1.3      cfgCsTerritoryPrimaryCluster
-- .2.1.3.1.1.2.1.4      cfgCsTerritoryBackupCluster
-- .2.1.3.1.2            cfgCsIntegrations
-- .2.1.3.1.2.1          cfgCsIntDirectoryService
-- .2.1.3.1.2.1.1        cfgCsIntDirSvcMSActiveDirectory
-- .2.1.3.1.2.1.1.1      cfgCsIntMSADEnabled
-- .2.1.3.1.2.1.1.2      cfgCsIntMSADResponsibleTerritory
-- .2.1.3.1.2.1.1.3      cfgCsIntMSADServerAddress
-- .2.1.3.1.2.1.1.4      cfgCsIntMSADUserId
-- .2.1.3.1.2.2          cfgCsIntCalendaring
-- .2.1.3.1.2.2.1        cfgCsIntCalMSExchange
-- .2.1.3.1.2.2.1.1      cfgCsIntMSExchEnabled
-- .2.1.3.1.2.2.1.2      cfgCsIntMSExchResponsibleTerritory
-- .2.1.3.1.2.2.1.3      cfgCsIntMSExchServerAddress
-- .2.1.3.1.2.2.1.4      cfgCsIntMSExchUserId
-- .2.1.3.1.2.3          cfgCsIntSiteTopology
-- .2.1.3.1.2.3.1        cfgCsIntSiteTopoPolycomCMA
-- .2.1.3.1.2.3.1.1      cfgCsIntPlcmCMAEnabled
-- .2.1.3.1.2.3.1.2      cfgCsIntPlcmCMAServerAddress
-- .2.1.3.1.2.3.1.3      cfgCsIntPlcmCMAUserId
-- .2.1.3.1.2.4          cfgCsIntNetwork
-- .2.1.3.1.2.4.1        cfgCsIntNetBandwidthManagement
-- .2.1.3.1.2.4.1.1      cfgCsIntNetBWMgmtJuniperSRC
-- .2.1.3.1.2.4.1.1.1    cfgCsIntJuniperSRCEnabled
-- .2.1.3.1.2.4.1.1.2    cfgCsIntJuniperSRCServerAddress
-- .2.1.3.1.2.4.1.1.3    cfgCsIntJuniperSRCServerPort
-- .2.1.3.1.2.4.1.1.4    cfgCsIntJuniperSRCUserId
-- .2.1.3.1.2.4.1.1.5    cfgCsIntJuniperSRCSubscriberURI
-- .2.1.3.2              cfgCsCluster
```

```
-- .2.1.3.2.1            cfgCsSignaling
-- .2.1.3.2.1.1          cfgCsSgnlH323
-- .2.1.3.2.1.1.1        cfgCsSgnlH323Enabled
-- .2.1.3.2.1.1.2        cfgCsSgnlH323H225Port
-- .2.1.3.2.1.1.3        cfgCsSgnlH323RASPort
-- .2.1.3.2.1.2          cfgCsSgnlSIP
-- .2.1.3.2.1.2.1        cfgCsSgnlSIPEnabled
-- .2.1.3.2.1.2.2        cfgCsSgnlSIPTCPPort
-- .2.1.3.2.1.2.3        cfgCsSgnlSIPUDPPort
-- .2.1.3.2.1.2.4        cfgCsSgnlSIPTLSPort
-- .2.1.4                cfgDevices
-- .2.2                  dmaStatus
-- .2.2.1                stServers
-- .2.2.1.1              stServerCount
-- .2.2.1.2              stIdentity
-- .2.2.1.2.1            stHardwareInfoTable
-- .2.2.1.2.1.1          stHardwareInfoEntry
-- .2.2.1.2.1.1.1        stHWIndex
-- .2.2.1.2.1.1.2        stHWHostName
-- .2.2.1.2.1.1.3        stHWSerialNumber
-- .2.2.1.2.2            stVersionTable
-- .2.2.1.2.2.1          stVersionEntry
-- .2.2.1.2.2.1.1        stVerIndex
-- .2.2.1.2.2.1.2        stVerHostName
-- .2.2.1.2.2.1.3        stVerVersion
-- .2.2.1.2.3            stSystemInfoTable
-- .2.2.1.2.3.1          stSystemInfoEntry
-- .2.2.1.2.3.1.1        stSysInfoIndex
-- .2.2.1.2.3.1.2        stSysInfoHostName
-- .2.2.1.2.3.1.3        stSysInfoSystemDate
-- .2.2.1.2.3.1.4        stSysInfoUptime
-- .2.2.1.2.3.1.5        stSysInfoTimeSource
-- .2.2.1.3              stNetwork
-- .2.2.1.3.1            stNetClusterAffiliationTable
-- .2.2.1.3.1.1          stNetClusterAffiliationEntry
-- .2.2.1.3.1.1.1        stNetClusterAffilIndex
-- .2.2.1.3.1.1.2        stNetClusterAffilHostName
-- .2.2.1.3.1.1.3        stNetClusterAffilClusterName
-- .2.2.1.3.2            stNetPrivateInterfaceTable
-- .2.2.1.3.2.1          stNetPrivateInterfaceEntry
-- .2.2.1.3.2.1.1        stNetPvtIndex
-- .2.2.1.3.2.1.2        stNetPvtHostName
-- .2.2.1.3.2.1.3        stNetPvtInterfaceName
-- .2.2.1.3.2.1.4        stNetPvtLinkStatus
-- .2.2.1.3.2.1.5        stNetPvtMACAddress
-- .2.2.1.3.2.1.6        stNetPvtIPv4Address
-- .2.2.1.3.2.1.7        stNetPvtIPv6Address
-- .2.2.1.3.3            stNetManagementInterfaceTable
-- .2.2.1.3.3.1          stNetManagementInterfaceEntry
-- .2.2.1.3.3.1.1        stNetMgmtIndex
```

```
-- .2.2.1.3.3.1.2        stNetMgmtHostName
-- .2.2.1.3.3.1.3        stNetMgmtInterfaceName
-- .2.2.1.3.3.1.4        stNetMgmtLinkStatus
-- .2.2.1.3.3.1.5        stNetMgmtMACAddress
-- .2.2.1.3.3.1.6        stNetMgmtIPv4Address
-- .2.2.1.3.3.1.7        stNetMgmtIPv6Address
-- .2.2.1.3.4            stNetSignalingInterfaceTable
-- .2.2.1.3.4.1          stNetSignalingInterfaceEntry
-- .2.2.1.3.4.1.1        stNetSgnlIndex
-- .2.2.1.3.4.1.2        stNetSgnlHostName
-- .2.2.1.3.4.1.3        stNetSgnlInterfaceName
-- .2.2.1.3.4.1.4        stNetSgnlLinkStatus
-- .2.2.1.3.4.1.5        stNetSgnlMACAddress
-- .2.2.1.3.4.1.6        stNetSgnlIPv4Address
-- .2.2.1.3.4.1.7        stNetSgnlIPv6Address
-- .2.2.1.4              stResources
-- .2.2.1.4.1            stRsrcCPUUsageTable
-- .2.2.1.4.1.1          stRsrcCPUUsageEntry
-- .2.2.1.4.1.1.1        stRsrcCPUUsageIndex
-- .2.2.1.4.1.1.2        stRsrcCPUUsageHostName
-- .2.2.1.4.1.1.3        stRsrcCPUUsageCPUUtilizationPct
-- .2.2.1.4.2            stRsrcMemoryUsageTable
-- .2.2.1.4.2.1          stRsrcMemoryUsageEntry
-- .2.2.1.4.2.1.1        stRsrcMemUsageIndex
-- .2.2.1.4.2.1.2        stRsrcMemUsageHostName
-- .2.2.1.4.2.1.3        stRsrcMemUsageTotalMemory
-- .2.2.1.4.2.1.4        stRsrcMemUsageBuffersAndCache
-- .2.2.1.4.2.1.5        stRsrcMemUsageUsed
-- .2.2.1.4.2.1.6        stRsrcMemUsageFree
-- .2.2.1.4.3            stRsrcSwapSpaceTable
-- .2.2.1.4.3.1          stRsrcSwapSpaceEntry
-- .2.2.1.4.3.1.1        stRsrcSwapIndex
-- .2.2.1.4.3.1.2        stRsrcSwapHostName
-- .2.2.1.4.3.1.3        stRsrcSwapTotal
-- .2.2.1.4.3.1.4        stRsrcSwapUsed
-- .2.2.1.4.4            stRsrcDiskSpaceTable
-- .2.2.1.4.4.1          stRsrcDiskSpaceEntry
-- .2.2.1.4.4.1.1        stRsrcDiskIndex
-- .2.2.1.4.4.1.2        stRsrcDiskHostName
-- .2.2.1.4.4.1.3        stRsrcDiskTotal
-- .2.2.1.4.4.1.4        stRsrcDiskUsed
-- .2.2.1.4.5            stRsrcLogSpaceTable
-- .2.2.1.4.5.1          stRsrcLogSpaceEntry
-- .2.2.1.4.5.1.1        stRsrcLogIndex
-- .2.2.1.4.5.1.2        stRsrcLogHostName
-- .2.2.1.4.5.1.3        stRsrcLogTotal
-- .2.2.1.4.5.1.4        stRsrcLogUsed
-- .2.2.1.4.5.1.5        stRsrcLogWarningThreshold
-- .2.2.1.4.5.1.6        stRsrcLogNextPurge
-- .2.2.2                stDevices
```

```
--  .2.2.2.1                stMCUs
--  .2.2.2.1.1              stMCUCount
--  .2.2.2.1.2              stMCUStatusTable
--  .2.2.2.1.2.1            stMCUStatusEntry
--  .2.2.2.1.2.1.1          stMCUStIndex
--  .2.2.2.1.2.1.2          stMCUStName
--  .2.2.2.1.2.1.3          stMCUStServiceStatus
--  .2.2.2.1.2.1.4          stMCUStHasAlert
--  .2.2.2.1.2.1.5          stMCUStRecordingAvailable
--  .2.2.2.1.2.1.6          stMCUStIVRAvailable
--  .2.2.2.1.3              stMCUVideoPortUsageTable
--  .2.2.2.1.3.1            stMCUVideoPortUsageEntry
--  .2.2.2.1.3.1.1          stMCUVidUsageIndex
--  .2.2.2.1.3.1.2          stMCUVidUsageName
--  .2.2.2.1.3.1.3          stMCUVidUsageMCUTotal
--  .2.2.2.1.3.1.4          stMCUVidUsageMCUUsed
--  .2.2.2.1.3.1.5          stMCUVidUsageDMATotal
--  .2.2.2.1.3.1.6          stMCUVidUsageDMAUsed
--  .2.2.2.1.3.1.7          stMCUVidUsageCMAReserved
--  .2.2.2.1.4              stMCUVoicePortUsageTable
--  .2.2.2.1.4.1            stMCUVoicePortUsageEntry
--  .2.2.2.1.4.1.1          stMCUVoxUsageIndex
--  .2.2.2.1.4.1.2          stMCUVoxUsageName
--  .2.2.2.1.4.1.3          stMCUVoxUsageMCUTotal
--  .2.2.2.1.4.1.4          stMCUVoxUsageMCUUsed
--  .2.2.2.1.4.1.5          stMCUVoxUsageDMATotal
--  .2.2.2.1.4.1.6          stMCUVoxUsageDMAUsed
--  .2.2.2.2                stMCUsPerCluster
--  .2.2.2.2.1              stMCUsPerClusterCount
--  .2.2.2.2.2              stMCUPCConnectionStatusTable
--  .2.2.2.2.2.1            stMCUPCConnectionStatusEntry
--  .2.2.2.2.2.1.1          stMCUPCConnStIndex
--  .2.2.2.2.2.1.2          stMCUPCConnStName
--  .2.2.2.2.2.1.3          stMCUPCConnStClusterName
--  .2.2.2.2.2.1.4          stMCUPCConnStConnectionStatus
--  .2.2.2.2.3              stMCUPCReliabilityStatsTable
--  .2.2.2.2.3.1            stMCUPCReliabilityStatsEntry
--  .2.2.2.2.3.1.1          stMCUPCRelIndex
--  .2.2.2.2.3.1.2          stMCUPCRelName
--  .2.2.2.2.3.1.3          stMCUPCRelClusterName
--  .2.2.2.2.3.1.4          stMCUPCRelDisconnects
--  .2.2.2.2.3.1.5          stMCUPCRelCallFailureRate
--  .2.2.3                  stClusters
--  .2.2.3.1                stClustersCount
--  .2.2.3.2                stClustersTable
--  .2.2.3.2.1              stClustersEntry
--  .2.2.3.2.1.1            stClIndex
--  .2.2.3.2.1.2            stClClusterName
--  .2.2.3.2.1.3            stClClusterStatus
--  .2.2.3.3                stLicensesTable
```

```
-- .2.2.3.3.1            stLicensesEntry
-- .2.2.3.3.1.1          stLicIndex
-- .2.2.3.3.1.2          stLicClusterName
-- .2.2.3.3.1.3          stLicLicenseStatus
-- .2.2.3.3.1.4          stLicLicensedCalls
-- .2.2.3.3.1.5          stLicCallserverActiveCalls
-- .2.2.4                stCallserver
-- .2.2.4.1              stCsSupercluster
-- .2.2.4.1.1            stCsSiteTopology
-- .2.2.4.1.1.1          stCsConfMgrTerritoriesCount
-- .2.2.4.1.1.2          stCsConfMgrTerritoriesTable
-- .2.2.4.1.1.2.1        stCsConfMgrTerritoriesEntry
-- .2.2.4.1.1.2.1.1      stCsConfMgrTerrIndex
-- .2.2.4.1.1.2.1.2      stCsConfMgrTerrName
-- .2.2.4.1.2            stCsIntegrations
-- .2.2.4.1.2.1          stCsIntDirectoryService
-- .2.2.4.1.2.1.1        stCsIntDirSvcMSActiveDirectory
-- .2.2.4.1.2.1.1.1      stCsIntMSADEnabled
-- .2.2.4.1.2.1.1.2      stCsIntMSADCacheStatus
-- .2.2.4.1.2.1.1.3      stCsIntMSADCachingCluster
-- .2.2.4.1.2.1.1.4      stCsIntMSADCachingServer
-- .2.2.4.1.2.1.1.5      stCsIntMSADConnectionSecure
-- .2.2.4.1.2.1.1.6      stCsIntMSADCacheRefreshDate
-- .2.2.4.1.2.1.1.7      stCsIntMSADEnterpriseConfRooms
-- .2.2.4.1.2.2          stCsIntCalendaring
-- .2.2.4.1.2.2.1        stCsIntCalMSExchange
-- .2.2.4.1.2.2.1.1      stCsIntMSExchEnabled
-- .2.2.4.1.2.2.1.2      stCsIntMSExchSubscriptionStatus
-- .2.2.4.1.2.2.1.3      stCsIntMSExchIntegratingCluster
-- .2.2.4.1.2.2.1.4      stCsIntMSExchIntegratingServer
-- .2.2.4.1.2.2.1.5      stCsIntMSExchMailbox
-- .2.2.4.1.2.2.1.6      stCsIntMSExchMeetingsToday
-- .2.2.4.1.2.3          stCsIntSiteTopology
-- .2.2.4.1.2.3.1        stCsIntSiteTopoPolycomCMA
-- .2.2.4.1.2.3.1.1      stCsIntPlcmCMAEnabled
-- .2.2.4.1.2.3.1.2      stCsIntPlcmCMAConnectionStatus
-- .2.2.4.1.2.3.1.3      stCsIntPlcmCMALastContactDate
-- .2.2.4.1.2.3.1.4      stCsIntPlcmCMATimeSinceLastRefresh
-- .2.2.4.1.2.3.1.5      stCsIntPlcmCMATerritories
-- .2.2.4.1.2.3.1.6      stCsIntPlcmCMASites
-- .2.2.4.1.2.3.1.7      stCsIntPlcmCMASiteLinks
-- .2.2.4.1.2.3.1.8      stCsIntPlcmCMAMPLSClouds
-- .2.2.4.1.2.4          stCsIntNetwork
-- .2.2.4.1.2.4.1        stCsIntNetBandwidthManagement
-- .2.2.4.1.2.4.1.1      stCsIntNetBWMgmtJuniperSRC
-- .2.2.4.1.2.4.1.1.1    stCsIntJuniperSRCEnabled
-- .2.2.4.2              stCsDevices
-- .2.2.4.2.1            stCsConfMgrMCUs
-- .2.2.4.2.1.1          stCsConfMgrMCUsCount
-- .2.2.4.2.1.2          stCsConfMgrMCUsTable
```

```
-- .2.2.4.2.1.2.1        stCsConfMgrMCUsEntry
-- .2.2.4.2.1.2.1.1      stCsCMMCUIndex
-- .2.2.4.2.1.2.1.2      stCsCMMCUName
-- .2.3                  dmaUsage
-- .2.3.1                useConfHistory
-- .2.3.1.1              useConfHistoryMaximumParticipants
-- .2.3.1.1.1            useCHMaxPartsLast60MinutesCount
-- .2.3.1.1.2            useCHMaxPartsLast60MinutesTable
-- .2.3.1.1.2.1          useCHMaxPartsLast60MinutesEntry
-- .2.3.1.1.2.1.1        useCHMaxParts60MinIndex
-- .2.3.1.1.2.1.2        useCHMaxParts60MinClusterName
-- .2.3.1.1.2.1.3        useCHMaxParts60MinTimestamp
-- .2.3.1.1.2.1.4        useCHMaxParts60MinMaxSimultaneousCalls
-- .2.3.1.1.2.1.5        useCHMaxParts60MinMaxAdHocCalls
-- .2.3.1.1.2.1.6        useCHMaxParts60MinMaxPCOCalls
-- .2.3.1.1.3            useCHMaxPartsLast24HoursCount
-- .2.3.1.1.4            useCHMaxPartsLast24HoursTable
-- .2.3.1.1.4.1          useCHMaxPartsLast24HoursEntry
-- .2.3.1.1.4.1.1        useCHMaxParts24HrIndex
-- .2.3.1.1.4.1.2        useCHMaxParts24HrClusterName
-- .2.3.1.1.4.1.3        useCHMaxParts24HrTimestamp
-- .2.3.1.1.4.1.4        useCHMaxParts24HrMaxSimultaneousCalls
-- .2.3.1.1.4.1.5        useCHMaxParts24HrMaxAdHocCalls
-- .2.3.1.1.4.1.6        useCHMaxParts24HrMaxPCOCalls
-- .2.3.1.1.5            useCHMaxPartsLast180DaysCount
-- .2.3.1.1.6            useCHMaxPartsLast180DaysTable
-- .2.3.1.1.6.1          useCHMaxPartsLast180DaysEntry
-- .2.3.1.1.6.1.1        useCHMaxParts180DaysIndex
-- .2.3.1.1.6.1.2        useCHMaxParts180DaysClusterName
-- .2.3.1.1.6.1.3        useCHMaxParts180DaysTimestamp
-- .2.3.1.1.6.1.4        useCHMaxParts180DaysMaxSimultaneousCalls
-- .2.3.1.1.6.1.5        useCHMaxParts180DaysMaxAdHocCalls
-- .2.3.1.1.6.1.6        useCHMaxParts180DaysMaxPCOCalls
-- .2.3.2                useCurrentConferences
-- .2.3.2.1              useCurrentConfsConfManagerUsage
-- .2.3.2.1.1            useConfMgrUsageCount
-- .2.3.2.1.2            useConfMgrUsageTable
-- .2.3.2.1.2.1          useConfMgrUsageEntry
-- .2.3.2.1.2.1.1        useCMUsageIndex
-- .2.3.2.1.2.1.2        useCMUsageClusterName
-- .2.3.2.1.2.1.3        useCMUsageActiveConfs
-- .2.3.2.1.2.1.4        useCMUsageActiveParts
-- .2.3.2.1.2.1.5        useCMUsageTotalVideoPorts
-- .2.3.2.1.2.1.6        useCMUsageUsedVideoPorts
-- .2.3.2.1.2.1.7        useCMUsageTotalVoicePorts
-- .2.3.2.1.2.1.8        useCMUsageUsedVoicePorts
-- .2.3.2.1.2.1.9        useCMUsageLocalUsers
-- .2.3.2.1.2.1.10       useCMUsageCustomConfRooms
-- .2.3.3                useDevices
-- .2.3.3.1              useDevRegistrations
```

```
-- .2.3.3.1.1          useDevRegistrationsCount
-- .2.3.3.1.2          useDevRegistrationsTable
-- .2.3.3.1.2.1        useDevRegistrationsEntry
-- .2.3.3.1.2.1.1      useDevRegIndex
-- .2.3.3.1.2.1.2      useDevRegClusterName
-- .2.3.3.1.2.1.3      useDevRegActiveEndpointReg
-- .2.3.3.1.2.1.4      useDevRegInactiveEndpointReg
-- .2.3.3.1.2.1.5      useDevRegFailedEndpointRegLast24Hours
-- .2.4                dmaAlerts
-- .2.4.1              alActiveAlerts
-- .2.4.1.1            alActiveAlertsCount
-- .2.4.1.2            alActiveAlertsTable
-- .2.4.1.2.1          alActiveAlertsEntry
-- .2.4.1.2.1.1        alActAlertIndex
-- .2.4.1.2.1.2        alActAlertID
-- .2.4.1.2.1.3        alActAlertTimestamp
-- .2.4.1.2.1.4        alActAlertCode
-- .2.4.1.2.1.5        alActAlertSeverity
-- .2.4.1.2.1.6        alActAlertDescription
-- .2.5                dmaNotifications
-- .2.5.1              ntfObjects
-- .2.5.1.1            ntfObjAlertID
-- .2.5.1.2            ntfObjAlertTimestamp
-- .2.5.1.3            ntfObjAlertCode
-- .2.5.1.4            ntfObjAlertSeverity
-- .2.5.1.5            ntfObjAlertDescription
-- .2.5.2              ntfAlertNotifications
-- .2.5.2.0            ntfAlertNotificationObjects
-- .2.5.2.0.1001       ntfAlertClusterBusyOut
-- .2.5.2.0.1002       ntfAlertClusterOutOfService
-- .2.5.2.0.1003       ntfAlertClusterOrphan
-- .2.5.2.0.1004       ntfAlertClusterUnreachable
-- .2.5.2.0.1005       ntfAlertClusterPendingReplication
-- .2.5.2.0.1101       ntfAlertTerritoryNotActiveBothClustersNotInService
-- .2.5.2.0.1102       ntfAlertTerritoryNotActiveClusterNotInService
-- .2.5.2.0.1103       ntfAlertTerritoryNoClustersAssigned
-- .2.5.2.0.1104       ntfAlertTerritoryPrimaryClusterNotInService
-- .2.5.2.0.2001       ntfAlertCMAUser
-- .2.5.2.0.2002       ntfAlertCMAUnreachable
-- .2.5.2.0.2101       ntfAlertEntDirIntegrationFailed
-- .2.5.2.0.2102       ntfAlertEntDirNoConfRooms
-- .2.5.2.0.2103       ntfAlertEntDirPrimaryClusterNotInService
-- .2.5.2.0.2104       ntfAlertEntDirNotAvailable
-- .2.5.2.0.2105       ntfAlertEntDirNotAvailableNoBackup
-- .2.5.2.0.2106       ntfAlertEntDirUserAuthConnectionFailed
-- .2.5.2.0.2107       ntfAlertEntDirCachingConnectionFailed
-- .2.5.2.0.2201       ntfAlertExchangePrimaryClusterNotInServiceBackupAvailable
-- .2.5.2.0.2202       ntfAlertExchangeBothClustersNotInService
-- .2.5.2.0.2203       ntfAlertExchangePrimaryClusterNotInService
-- .2.5.2.0.3001       ntfAlertSignalingNotEnabled
```

```
--  .2.5.2.0.3101          ntfAlertCertExpired
--  .2.5.2.0.3102          ntfAlertCertExpireNow
--  .2.5.2.0.3103          ntfAlertCertExpireSoon
--  .2.5.2.0.3104          ntfAlertCertSecExpired
--  .2.5.2.0.3105          ntfAlertCertSecExpireSoon
--  .2.5.2.0.3201          ntfAlertLicenseNoKeys
--  .2.5.2.0.3202          ntfAlertLicenseInvalidKeys
--  .2.5.2.0.3301          ntfAlertNetworkSingleNodeDetected
--  .2.5.2.0.3302          ntfAlertNetworkPrivateActive
--  .2.5.2.0.3303          ntfAlertNetworkPrivateError
--  .2.5.2.0.3304          ntfAlertNetworkPublicError
--  .2.5.2.0.3305          ntfAlertNetworkSignalingError
--  .2.5.2.0.3401          ntfAlertResourceDiskSpace
--  .2.5.2.0.3402          ntfAlertResourceLogsPurge
--  .2.5.2.0.3403          ntfAlertResourceLogsExceedLimit
--  .2.5.2.0.3404          ntfAlertResourceLogsNearLimit
--  .2.5.2.0.3405          ntfAlertResourceCPUOver50Percent
--  .2.5.2.0.3406          ntfAlertResourceCPUOver75Percent
--  .2.5.2.0.3501          ntfAlertAVVirusDetected
--  .2.5.2.0.3502          ntfAlertAVUnsuccessful
--  .2.5.2.0.3503          ntfAlertAVNeverSucceeded
--  .2.5.2.0.3601          ntfAlertDataSyncVersion
--  .2.5.2.0.3602          ntfAlertDataSyncSystemTime
--  .2.5.2.0.3603          ntfAlertDataSyncADIntegration
--  .2.5.2.0.3604          ntfAlertDataSyncADConfRooms
--  .2.5.2.0.3605          ntfAlertDataSyncCustomConfRooms
--  .2.5.2.0.3606          ntfAlertDataSyncLocalUsers
--  .2.5.2.0.4001          ntfAlertMCUBusyOut
--  .2.5.2.0.4002          ntfAlertMCUOutOfService
--  .2.5.2.0.4003          ntfAlertMCUMultipleWarnings
--  .2.5.2.0.5001          ntfAlertITPSystemConfigurationError
--  .2.5.2.0.5002ntfAlertEndpointSignalingAlert
--  .2.5.2.0.6001          ntfAlertConfMgrNoTerritories
--  .2.5.2.0.7001          ntfAlertCallServerRegistrationDataIncomplete
--  .2.9                   dmaConformance
--  .2.9.1                 dmaConformanceGroups
--  .2.9.1.1               dmaConformanceConfig
--  .2.9.1.2               dmaConformanceStatus
--  .2.9.1.3               dmaConformanceUsage
--  .2.9.1.4               dmaConformanceAlerts
--  .2.9.1.5               dmaConformanceNotifications
--  .2.9.1.5.1             dmaConformanceNtfObjects
--  .2.9.1.5.2             dmaConformanceNtfAlertNotifications
--  .2.10                  dmaCompliance


IMPORTS
    TEXTUAL-CONVENTION, DisplayString, TruthValue, DateAndTime
        FROM SNMPv2-TC
    MODULE-IDENTITY, OBJECT-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
```

```
    Unsigned32, IpAddress, TimeTicks
        FROM SNMPv2-SMI
    OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    polycom
        FROM POLYCOM-BASE-MIB
;

dma MODULE-IDENTITY
    LAST-UPDATED    "201109220000Z"
    ORGANIZATION    "Polycom, Inc."
    CONTACT-INFO    "http://www.polycom.com/dma"
    DESCRIPTION     "This MIB defines the SNMP interface for monitoring the Polycom Distributed
Media
                    Application(tm) DMA(tm) 7000 system.
                    Copyright (c) 2011 Polycom, Inc."

    REVISION        "201109220000Z"
    DESCRIPTION     "Initial draft."

    ::= { polycom 13 }


-- TEXTUAL CONVENTIONS

GeneralString ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "512a"
    STATUS          current
    DESCRIPTION     "A typical string, up to 512 bytes in length."
    SYNTAX          OCTET STRING (SIZE (0..512))

Ipv6Address ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "39a"
    STATUS          current
    DESCRIPTION     "An IPv6 address, represented as a string."
    SYNTAX          OCTET STRING (SIZE (0..23))

PortNumber ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "d"
STATUS   current
DESCRIPTION   "A numbered network port."
SYNTAX   Unsigned32 (0..65535)

-- DMA

-- dma.1
dmaInternal1 OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "This OID is used within the internal processes of the DMA system and is not
provided
                for monitoring purposes."
```

```
   ::= { dma 1 }

-- dma.2
dmaMonitoring1 OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "This OID contains the DMA system's monitoring data exposed over SNMP."
   ::= { dma 2 }

-- DMA CONFIG

-- dma.2.1
dmaConfig OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Contains configuration data for the DMA system."
   ::= { dmaMonitoring1 1 }

-- dma.2.1.1
cfgIdentity OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Identification info for the server from which data is being retrieved."
   ::= { dmaConfig 1 }

-- dma.2.1.1.1
cfgProductInfo OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Information about the DMA product."
   ::= { cfgIdentity 1 }

-- dma.2.1.1.1.1
cfgProdInfoManufacturer OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Manufacturer of the DMA product."
   ::= { cfgProductInfo 1 }

-- dma.2.1.1.1.2
cfgProdInfoModel OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Model of the DMA product."
   ::= { cfgProductInfo 2 }

-- dma.2.1.1.1.3
cfgProdInfoHardwareInfo OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Information about the server's hardware."
   ::= { cfgProductInfo 3 }
```

```
-- dma.2.1.1.1.3.1
cfgProdInfoHWModel OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Server's hardware model."
    ::= { cfgProdInfoHardwareInfo 1 }


-- dma.2.1.1.1.3.2
cfgProdInfoHWSerialNumber OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Server's serial number (used for license keys)."
    ::= { cfgProdInfoHardwareInfo 2 }


-- dma.2.1.1.1.4
cfgProdInfoSoftwareInfo OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Information about the server's software."
    ::= { cfgProductInfo 4 }


-- dma.2.1.1.1.4.1
cfgProdInfoSWVersion OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The product's version."
    ::= { cfgProdInfoSoftwareInfo 1 }


-- dma.2.1.1.1.4.2
cfgProdInfoSWExtendedVersion OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Additional version information supplementary to the product version."
    ::= { cfgProdInfoSoftwareInfo 2 }


-- dma.2.1.1.1.4.2.1
cfgProdInfoSWExtVerPlatformVersion OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The version of the DMA application server (platform)."
    ::= { cfgProdInfoSWExtendedVersion 1 }


-- dma.2.1.1.1.4.2.2
cfgProdInfoSWExtVerApplicationVersion OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The version of the Ad-hoc Video server (application)."
```

```
    ::= { cfgProdInfoSWExtendedVersion 2 }

-- dma.2.1.2
cfgServer OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Configuration applied to the server from which data is being retrieved."
    ::= { dmaConfig 2 }

-- dma.2.1.2.1
cfgNetwork OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains info about the server's network settings."
    ::= { cfgServer 1 }

-- dma.2.1.2.1.1
cfgNetworkHostname OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The hostname configured for the server."
    ::= { cfgNetwork 1 }

-- dma.2.1.2.1.2
cfgInterfacesCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of indexed entries in cfgInterfacesTable."
    ::= { cfgNetwork 2 }

-- dma.2.1.2.1.3
cfgInterfacesTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CfgInterfacesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Specified network interfaces."
    ::= { cfgNetwork 3 }

-- dma.2.1.2.1.3.1
cfgInterfacesEntry OBJECT-TYPE
    SYNTAX      CfgInterfacesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in cfgInterfacesTable."
    INDEX       { cfgIfIndex }
    ::= { cfgInterfacesTable 1 }

CfgInterfacesEntry ::= SEQUENCE
{
    cfgIfIndex              Unsigned32,
```

```
    cfgIfName               GeneralString,
    cfgIfEnabled            TruthValue,
    cfgIfMACAddress         DisplayString,
    cfgIfIPv4Address        IpAddress,
    cfgIfIPv4SubnetMask     IpAddress,
    cfgIfIPv4Gateway        IpAddress,
    cfgIfIPv6Address        Ipv6Address,
    cfgIfIPv6PrefixLength   Unsigned32
}

-- dma.2.1.2.1.3.1.1
cfgIfIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "cfgInterfacesTable index."
    ::= { cfgInterfacesEntry 1 }

-- dma.2.1.2.1.3.1.2
cfgIfName OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the network interface."
    ::= { cfgInterfacesEntry 2 }

-- dma.2.1.2.1.3.1.3
cfgIfEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if network configuration utilizes this interface."
    ::= { cfgInterfacesEntry 3 }

-- dma.2.1.2.1.3.1.4
cfgIfMACAddress OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "MAC address for this interface."
    ::= { cfgInterfacesEntry 4 }

-- dma.2.1.2.1.3.1.5
cfgIfIPv4Address OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "IPv4 address assigned to this interface."
    ::= { cfgInterfacesEntry 5 }
```

```
-- dma.2.1.2.1.3.1.6
cfgIfIPv4SubnetMask OBJECT-TYPE
    SYNTAX        IpAddress
    MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION "IPv4 subnet mask assigned to this interface."
    ::= { cfgInterfacesEntry 6 }


-- dma.2.1.2.1.3.1.7
cfgIfIPv4Gateway OBJECT-TYPE
    SYNTAX        IpAddress
    MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION "IPv4 gateway assigned to this interface."
    ::= { cfgInterfacesEntry 7 }


-- dma.2.1.2.1.3.1.8
cfgIfIPv6Address OBJECT-TYPE
    SYNTAX        Ipv6Address
    MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION "IPv6 address assigned to this interface."
    ::= { cfgInterfacesEntry 8 }


-- dma.2.1.2.1.3.1.9
cfgIfIPv6PrefixLength OBJECT-TYPE
    SYNTAX        Unsigned32
    MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION "IPv6 prefix assigned to this interface."
    ::= { cfgInterfacesEntry 9 }


-- dma.2.1.3
cfgCallserver OBJECT-IDENTITY
    STATUS        current
    DESCRIPTION "Configuration for the DMA call server."
    ::= { dmaConfig 3 }


-- dma.2.1.3.1
cfgCsSupercluster OBJECT-IDENTITY
    STATUS        current
    DESCRIPTION "Call server configuration common to any supercluster member."
    ::= { cfgCallserver 1 }


-- dma.2.1.3.1.1
cfgCsSiteTopology OBJECT-IDENTITY
    STATUS        current
    DESCRIPTION "Site topology configuration for the call server."
    ::= { cfgCsSupercluster 1 }
```

```
-- dma.2.1.3.1.1.1
cfgCsTerritoriesCount OBJECT-TYPE
    SYNTAX        Unsigned32
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION "Number of indexed entries in cfgCsTerritoriesTable."
    ::= { cfgCsSiteTopology 1 }


-- dma.2.1.3.1.1.2
cfgCsTerritoriesTable OBJECT-TYPE
    SYNTAX        SEQUENCE OF CfgCsTerritoriesEntry
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION "Configured territories."
    ::= { cfgCsSiteTopology 2 }


-- dma.2.1.3.1.1.2.1
cfgCsTerritoriesEntry OBJECT-TYPE
    SYNTAX        CfgCsTerritoriesEntry
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION "An entry in cfgCsTerritoriesTable."
    INDEX        { cfgCsTerritoryIndex }
    ::= { cfgCsTerritoriesTable 1 }


CfgCsTerritoriesEntry ::= SEQUENCE
{
    cfgCsTerritoryIndex          Unsigned32,
    cfgCsTerritoryName           GeneralString,
    cfgCsTerritoryPrimaryCluster GeneralString,
    cfgCsTerritoryBackupCluster  GeneralString
}

-- dma.2.1.3.1.1.2.1.1
cfgCsTerritoryIndex OBJECT-TYPE
    SYNTAX        Unsigned32
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION "cfgCsTerritoriesTable index."
    ::= { cfgCsTerritoriesEntry 1 }


-- dma.2.1.3.1.1.2.1.2
cfgCsTerritoryName OBJECT-TYPE
    SYNTAX        GeneralString
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION "Name of the territory."
    ::= { cfgCsTerritoriesEntry 2 }


-- dma.2.1.3.1.1.2.1.3
```

```
cfgCsTerritoryPrimaryCluster OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Cluster assigned primary responsibility for this territory."
   ::= { cfgCsTerritoriesEntry 3 }


-- dma.2.1.3.1.1.2.1.4
cfgCsTerritoryBackupCluster OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Cluster assigned backup responsibility for this territory."
   ::= { cfgCsTerritoriesEntry 4 }


-- dma.2.1.3.1.2
cfgCsIntegrations OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Configurations for systems with which the DMA integrates."
   ::= { cfgCsSupercluster 2 }


-- dma.2.1.3.1.2.1
cfgCsIntDirectoryService OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Configurations for directory service integration."
   ::= { cfgCsIntegrations 1 }


-- dma.2.1.3.1.2.1.1
cfgCsIntDirSvcMSActiveDirectory OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Configuration for Microsoft Active Directory integration."
   ::= { cfgCsIntDirectoryService 1 }


-- dma.2.1.3.1.2.1.1.1
cfgCsIntMSADEnabled OBJECT-TYPE
   SYNTAX       TruthValue
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "True if Active Directory integration is enabled."
   ::= { cfgCsIntDirSvcMSActiveDirectory 1 }


-- dma.2.1.3.1.2.1.1.2
cfgCsIntMSADResponsibleTerritory OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Name of the territory responsible for Active Directory integration."
   ::= { cfgCsIntDirSvcMSActiveDirectory 2 }


-- dma.2.1.3.1.2.1.1.3
```

```
cfgCsIntMSADServerAddress OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Address of the Active Directory server."
   ::= { cfgCsIntDirSvcMSActiveDirectory 3 }


-- dma.2.1.3.1.2.1.1.4
cfgCsIntMSADUserId OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "User ID of the service account used to integrate with Active Directory."
   ::= { cfgCsIntDirSvcMSActiveDirectory 4 }


-- dma.2.1.3.1.2.2
cfgCsIntCalendaring OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Configurations for calendaring service integration."
   ::= { cfgCsIntegrations 2 }


-- dma.2.1.3.1.2.2.1
cfgCsIntCalMSExchange OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Configuration for Microsoft Exchange Server integration."
   ::= { cfgCsIntCalendaring 1 }


-- dma.2.1.3.1.2.2.1.1
cfgCsIntMSExchEnabled OBJECT-TYPE
   SYNTAX       TruthValue
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "True if Exchange integration is enabled."
   ::= { cfgCsIntCalMSExchange 1 }


-- dma.2.1.3.1.2.2.1.2
cfgCsIntMSExchResponsibleTerritory OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Name of the territory responsible for Exchange integration."
   ::= { cfgCsIntCalMSExchange 2 }


-- dma.2.1.3.1.2.2.1.3
cfgCsIntMSExchServerAddress OBJECT-TYPE
   SYNTAX       GeneralString
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Address of the Exchange server."
   ::= { cfgCsIntCalMSExchange 3 }
```

```
-- dma.2.1.3.1.2.2.1.4
cfgCsIntMSExchUserId OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "User ID of the service account used to integrate with Exchange."
   ::= { cfgCsIntCalMSExchange 4 }


-- dma.2.1.3.1.2.3
cfgCsIntSiteTopology OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Configurations for site topology service integration."
   ::= { cfgCsIntegrations 3 }


-- dma.2.1.3.1.2.3.1
cfgCsIntSiteTopoPolycomCMA OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Configuration for Polycom CMA system integration."
   ::= { cfgCsIntSiteTopology 1 }


-- dma.2.1.3.1.2.3.1.1
cfgCsIntPlcmCMAEnabled OBJECT-TYPE
   SYNTAX      TruthValue
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "True if CMA integration is enabled."
   ::= { cfgCsIntSiteTopoPolycomCMA 1 }


-- dma.2.1.3.1.2.3.1.2
cfgCsIntPlcmCMAServerAddress OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Address of the CMA system."
   ::= { cfgCsIntSiteTopoPolycomCMA 2 }


-- dma.2.1.3.1.2.3.1.3
cfgCsIntPlcmCMAUserId OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "User ID of the service account used to integrate with the CMA system."
   ::= { cfgCsIntSiteTopoPolycomCMA 3 }


-- dma.2.1.3.1.2.4
cfgCsIntNetwork OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Configurations for network integrations."
   ::= { cfgCsIntegrations 4 }
```

```
-- dma.2.1.3.1.2.4.1
cfgCsIntNetBandwidthManagement OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Configurations for bandwidth management integrations."
    ::= { cfgCsIntNetwork 1 }


-- dma.2.1.3.1.2.4.1.1
cfgCsIntNetBWMgmtJuniperSRC OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Configuration for Juniper Networks SRC integration."
    ::= { cfgCsIntNetBandwidthManagement 1 }


-- dma.2.1.3.1.2.4.1.1.1
cfgCsIntJuniperSRCEnabled OBJECT-TYPE
    SYNTAX       TruthValue
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "True if Juniper SRC integration is enabled."
    ::= { cfgCsIntNetBWMgmtJuniperSRC 1 }


-- dma.2.1.3.1.2.4.1.1.2
cfgCsIntJuniperSRCServerAddress OBJECT-TYPE
    SYNTAX       GeneralString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Address of the Juniper SRC server."
    ::= { cfgCsIntNetBWMgmtJuniperSRC 2 }


-- dma.2.1.3.1.2.4.1.1.3
cfgCsIntJuniperSRCServerPort OBJECT-TYPE
    SYNTAX       PortNumber
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Connection port of the Juniper SRC server."
    ::= { cfgCsIntNetBWMgmtJuniperSRC 3 }


-- dma.2.1.3.1.2.4.1.1.4
cfgCsIntJuniperSRCUserId OBJECT-TYPE
    SYNTAX       GeneralString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "User ID of the service account used to connect to the Juniper SRC server."
    ::= { cfgCsIntNetBWMgmtJuniperSRC 4 }


-- dma.2.1.3.1.2.4.1.1.5
cfgCsIntJuniperSRCSubscriberURI OBJECT-TYPE
    SYNTAX       GeneralString
    MAX-ACCESS   read-only
    STATUS       current
```

```
    DESCRIPTION "URI used for the Juniper SRC server connection."
    ::= { cfgCsIntNetBWMgmtJuniperSRC 5 }

-- dma.2.1.3.2
cfgCsCluster OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Call server configuration specific to the cluster from which data is being
retrieved."
    ::= { cfgCallserver 2 }

-- dma.2.1.3.2.1
cfgCsSignaling OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Signaling configuration for the cluster."
    ::= { cfgCsCluster 1 }

-- dma.2.1.3.2.1.1
cfgCsSgnlH323 OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "H.323 signaling configuration for the cluster."
    ::= { cfgCsSignaling 1 }

-- dma.2.1.3.2.1.1.1
cfgCsSgnlH323Enabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if H.323 signaling is enabled."
    ::= { cfgCsSgnlH323 1 }

-- dma.2.1.3.2.1.1.2
cfgCsSgnlH323H225Port OBJECT-TYPE
    SYNTAX      PortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The configured H.225 port."
    ::= { cfgCsSgnlH323 2 }

-- dma.2.1.3.2.1.1.3
cfgCsSgnlH323RASPort OBJECT-TYPE
    SYNTAX      PortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The configured RAS port."
    ::= { cfgCsSgnlH323 3 }

-- dma.2.1.3.2.1.2
cfgCsSgnlSIP OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "SIP signaling configuration for the cluster."
```

```
    ::= { cfgCsSignaling 2 }


-- dma.2.1.3.2.1.2.1
cfgCsSgnlSIPEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if SIP signaling is enabled."
    ::= { cfgCsSgnlSIP 1 }


-- dma.2.1.3.2.1.2.2
cfgCsSgnlSIPTCPPort OBJECT-TYPE
    SYNTAX      PortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The configured TCP transport SIP port."
    ::= { cfgCsSgnlSIP 2 }


-- dma.2.1.3.2.1.2.3
cfgCsSgnlSIPUDPPort OBJECT-TYPE
    SYNTAX      PortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The configured UDP transport SIP port."
    ::= { cfgCsSgnlSIP 3 }


-- dma.2.1.3.2.1.2.4
cfgCsSgnlSIPTLSPort OBJECT-TYPE
    SYNTAX      PortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The configured TLS transport SIP port."
    ::= { cfgCsSgnlSIP 4 }


-- dma.2.1.4
cfgDevices OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Configuration for devices connecting to the DMA call server."
    ::= { dmaConfig 4 }


-- DMA STATUS


-- dma.2.2
dmaStatus OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains status data for the DMA system."
    ::= { dmaMonitoring1 2 }


-- dma.2.2.1
stServers OBJECT-IDENTITY
```

Polycom, Inc.   463

```
   STATUS       current
   DESCRIPTION "Status of DMA servers."
   ::= { dmaStatus 1 }


-- dma.2.2.1.1
stServerCount OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of indexed entries in the tables within stServers."
   ::= { stServers 1 }


-- dma.2.2.1.2
stIdentity OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Server identity statuses."
   ::= { stServers 2 }


-- dma.2.2.1.2.1
stHardwareInfoTable OBJECT-TYPE
   SYNTAX       SEQUENCE OF StHardwareInfoEntry
   MAX-ACCESS  not-accessible
   STATUS       current
   DESCRIPTION "Server hardware identification."
   ::= { stIdentity 1 }


-- dma.2.2.1.2.1.1
stHardwareInfoEntry OBJECT-TYPE
   SYNTAX       StHardwareInfoEntry
   MAX-ACCESS  not-accessible
   STATUS       current
   DESCRIPTION "An entry in stHardwareInfoTable."
   INDEX        { stHWIndex }
   ::= { stHardwareInfoTable 1 }

StHardwareInfoEntry ::= SEQUENCE
{
   stHWIndex         Unsigned32,
   stHWHostName      DisplayString,
   stHWSerialNumber  GeneralString
}

-- dma.2.2.1.2.1.1.1
stHWIndex OBJECT-TYPE
   SYNTAX    Unsigned32
   MAX-ACCESS  not-accessible
   STATUS       current
   DESCRIPTION "stHardwareInfoTable index."
   ::= { stHardwareInfoEntry 1 }
```

```
-- dma.2.2.1.2.1.1.2
stHWHostName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of the server."
   ::= { stHardwareInfoEntry 2 }


-- dma.2.2.1.2.1.1.3
stHWSerialNumber OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Server's serial number."
   ::= { stHardwareInfoEntry 3 }


-- dma.2.2.1.2.2
stVersionTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StVersionEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Server version information."
   ::= { stIdentity 2 }


-- dma.2.2.1.2.2.1
stVersionEntry OBJECT-TYPE
   SYNTAX      StVersionEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stVersionTable"
   INDEX       { stVerIndex }
   ::= { stVersionTable 1 }


StVersionEntry ::= SEQUENCE
{
   stVerIndex     Unsigned32,
   stVerHostName  DisplayString,
   stVerVersion   GeneralString
}

-- dma.2.2.1.2.2.1.1
stVerIndex OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stVersionTable index."
   ::= { stVersionEntry 1 }


-- dma.2.2.1.2.2.1.2
stVerHostName OBJECT-TYPE
```

```
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stVersionEntry 2 }


-- dma.2.2.1.2.2.1.3
stVerVersion OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Product version of the server."
   ::= { stVersionEntry 3 }


-- dma.2.2.1.2.3
stSystemInfoTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StSystemInfoEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Server statuses."
   ::= { stIdentity 3 }


-- dma.2.2.1.2.3.1
stSystemInfoEntry OBJECT-TYPE
   SYNTAX      StSystemInfoEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stSystemInfoTable."
   INDEX       { stSysInfoIndex }
   ::= { stSystemInfoTable 1 }


StSystemInfoEntry ::= SEQUENCE
{
   stSysInfoIndex       Unsigned32,
   stSysInfoHostName    DisplayString,
   stSysInfoSystemDate  DateAndTime,
   stSysInfoUptime      TimeTicks,
   stSysInfoTimeSource  INTEGER
}

-- dma.2.2.1.2.3.1.1
stSysInfoIndex OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stSystemInfoTable index."
   ::= { stSystemInfoEntry 1 }


-- dma.2.2.1.2.3.1.2
stSysInfoHostName OBJECT-TYPE
```

```
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stSystemInfoEntry 2 }


-- dma.2.2.1.2.3.1.3
stSysInfoSystemDate OBJECT-TYPE
   SYNTAX      DateAndTime
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Server's current system date."
   ::= { stSystemInfoEntry 3 }


-- dma.2.2.1.2.3.1.4
stSysInfoUptime OBJECT-TYPE
   SYNTAX      TimeTicks
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "How long the server has been powered up."
   ::= { stSystemInfoEntry 4 }


-- dma.2.2.1.2.3.1.5
stSysInfoTimeSource OBJECT-TYPE
   SYNTAX      INTEGER
               { internal(1), external(2) }
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Server's source for time synchronization - internal/external."
   ::= { stSystemInfoEntry 5 }


-- dma.2.2.1.3
stNetwork OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Server network statuses."
   ::= { stServers 3 }


-- dma.2.2.1.3.1
stNetClusterAffiliationTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StNetClusterAffiliationEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Matches servers with the clusters to which they belong."
   ::= { stNetwork 1 }


-- dma.2.2.1.3.1.1
stNetClusterAffiliationEntry OBJECT-TYPE
   SYNTAX      StNetClusterAffiliationEntry
   MAX-ACCESS  not-accessible
   STATUS      current
```

```
   DESCRIPTION "An entry in stNetClusterAffiliationTable."
   INDEX       { stNetClusterAffilIndex }
   ::= { stNetClusterAffiliationTable 1 }

StNetClusterAffiliationEntry ::= SEQUENCE
{
   stNetClusterAffilIndex        Unsigned32,
   stNetClusterAffilHostName     DisplayString,
   stNetClusterAffilClusterName  DisplayString
}

-- dma.2.2.1.3.1.1.1
stNetClusterAffilIndex OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stNetClusterAffiliationTable index."
   ::= { stNetClusterAffiliationEntry 1 }

-- dma.2.2.1.3.1.1.2
stNetClusterAffilHostName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stNetClusterAffiliationEntry 2 }

-- dma.2.2.1.3.1.1.3
stNetClusterAffilClusterName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Cluster to which the server belongs."
   ::= { stNetClusterAffiliationEntry 3 }

-- dma.2.2.1.3.2
stNetPrivateInterfaceTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StNetPrivateInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Information about the private network interfaces of servers."
   ::= { stNetwork 2 }

-- dma.2.2.1.3.2.1
stNetPrivateInterfaceEntry OBJECT-TYPE
   SYNTAX      StNetPrivateInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stNetPrivateInterfaceTable."
   INDEX       { stNetPvtIndex }
```

```
    ::= { stNetPrivateInterfaceTable 1 }

StNetPrivateInterfaceEntry ::= SEQUENCE
{
    stNetPvtIndex          Unsigned32,
    stNetPvtHostName       DisplayString,
    stNetPvtInterfaceName  GeneralString,
    stNetPvtLinkStatus     INTEGER,
    stNetPvtMACAddress     DisplayString,
    stNetPvtIPv4Address    IpAddress,
    stNetPvtIPv6Address    Ipv6Address
}

-- dma.2.2.1.3.2.1.1
stNetPvtIndex OBJECT-TYPE
    SYNTAX     Unsigned32
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION "stNetPrivateInterfaceTable index."
    ::= { stNetPrivateInterfaceEntry 1 }

-- dma.2.2.1.3.2.1.2
stNetPvtHostName OBJECT-TYPE
    SYNTAX     DisplayString
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION "Hostname of the server."
    ::= { stNetPrivateInterfaceEntry 2 }

-- dma.2.2.1.3.2.1.3
stNetPvtInterfaceName OBJECT-TYPE
    SYNTAX     GeneralString
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION "Name of the network interface configured for private network."
    ::= { stNetPrivateInterfaceEntry 3 }

-- dma.2.2.1.3.2.1.4
stNetPvtLinkStatus OBJECT-TYPE
    SYNTAX     INTEGER
               { up(1), down(2) }
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION "Link status of the private network interface."
    ::= { stNetPrivateInterfaceEntry 4 }

-- dma.2.2.1.3.2.1.5
stNetPvtMACAddress OBJECT-TYPE
    SYNTAX     DisplayString
    MAX-ACCESS read-only
```

```
   STATUS      current
   DESCRIPTION "MAC address of the private network interface."
   ::= { stNetPrivateInterfaceEntry 5 }


-- dma.2.2.1.3.2.1.6
stNetPvtIPv4Address OBJECT-TYPE
   SYNTAX      IpAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv4 address assigned to the private network interface."
   ::= { stNetPrivateInterfaceEntry 6 }


-- dma.2.2.1.3.2.1.7
stNetPvtIPv6Address OBJECT-TYPE
   SYNTAX      Ipv6Address
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv6 address assigned to the private network interface."
   ::= { stNetPrivateInterfaceEntry 7 }


-- dma.2.2.1.3.3
stNetManagementInterfaceTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StNetManagementInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Information about the management network interfaces of servers."
   ::= { stNetwork 3 }


-- dma.2.2.1.3.3.1
stNetManagementInterfaceEntry OBJECT-TYPE
   SYNTAX      StNetManagementInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stNetManagementInterfaceTable."
   INDEX       { stNetMgmtIndex }
   ::= { stNetManagementInterfaceTable 1 }


StNetManagementInterfaceEntry ::= SEQUENCE
{
   stNetMgmtIndex          Unsigned32,
   stNetMgmtHostName       DisplayString,
   stNetMgmtInterfaceName  GeneralString,
   stNetMgmtLinkStatus     INTEGER,
   stNetMgmtMACAddress     DisplayString,
   stNetMgmtIPv4Address    IpAddress,
   stNetMgmtIPv6Address    Ipv6Address
}

-- dma.2.2.1.3.3.1.1
stNetMgmtIndex OBJECT-TYPE
```

```
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stNetManagementInterfaceTable index."
   ::= { stNetManagementInterfaceEntry 1 }


-- dma.2.2.1.3.3.1.2
stNetMgmtHostName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stNetManagementInterfaceEntry 2 }


-- dma.2.2.1.3.3.1.3
stNetMgmtInterfaceName OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of the network interface configured for management network."
   ::= { stNetManagementInterfaceEntry 3 }


-- dma.2.2.1.3.3.1.4
stNetMgmtLinkStatus OBJECT-TYPE
   SYNTAX      INTEGER
               { up(1), down(2) }
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Link status of the management network interface."
   ::= { stNetManagementInterfaceEntry 4 }


-- dma.2.2.1.3.3.1.5
stNetMgmtMACAddress OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "MAC address of the management network interface."
   ::= { stNetManagementInterfaceEntry 5 }


-- dma.2.2.1.3.3.1.6
stNetMgmtIPv4Address OBJECT-TYPE
   SYNTAX      IpAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv4 address assigned to the management network interface."
   ::= { stNetManagementInterfaceEntry 6 }


-- dma.2.2.1.3.3.1.7
stNetMgmtIPv6Address OBJECT-TYPE
   SYNTAX      Ipv6Address
```

```
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv6 address assigned to the management network interface."
   ::= { stNetManagementInterfaceEntry 7 }

-- dma.2.2.1.3.4
stNetSignalingInterfaceTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StNetSignalingInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Information about the signaling network interfaces of servers."
   ::= { stNetwork 4 }

-- dma.2.2.1.3.4.1
stNetSignalingInterfaceEntry OBJECT-TYPE
   SYNTAX      StNetSignalingInterfaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stNetSignalingInterfaceTable"
   INDEX       { stNetSgnlIndex }
   ::= { stNetSignalingInterfaceTable 1 }

StNetSignalingInterfaceEntry ::= SEQUENCE
{
   stNetSgnlIndex         Unsigned32,
   stNetSgnlHostName      DisplayString,
   stNetSgnlInterfaceName GeneralString,
   stNetSgnlLinkStatus    INTEGER,
   stNetSgnlMACAddress    DisplayString,
   stNetSgnlIPv4Address   IpAddress,
   stNetSgnlIPv6Address   Ipv6Address
}

-- dma.2.2.1.3.4.1.1
stNetSgnlIndex OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stNetSignalingInterfaceTable index."
   ::= { stNetSignalingInterfaceEntry 1 }

-- dma.2.2.1.3.4.1.2
stNetSgnlHostName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stNetSignalingInterfaceEntry 2 }

-- dma.2.2.1.3.4.1.3
```

```
stNetSgnlInterfaceName OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of the network interface configured for signaling network."
   ::= { stNetSignalingInterfaceEntry 3 }


-- dma.2.2.1.3.4.1.4
stNetSgnlLinkStatus OBJECT-TYPE
   SYNTAX      INTEGER
               { up(1), down(2) }
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Link status of the signaling network interface."
   ::= { stNetSignalingInterfaceEntry 4 }


-- dma.2.2.1.3.4.1.5
stNetSgnlMACAddress OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "MAC address of the signaling network interface."
   ::= { stNetSignalingInterfaceEntry 5 }


-- dma.2.2.1.3.4.1.6
stNetSgnlIPv4Address OBJECT-TYPE
   SYNTAX      IpAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv4 address assigned to the signaling network interface."
   ::= { stNetSignalingInterfaceEntry 6 }


-- dma.2.2.1.3.4.1.7
stNetSgnlIPv6Address OBJECT-TYPE
   SYNTAX      Ipv6Address
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "IPv6 address assigned to the signaling network interface."
   ::= { stNetSignalingInterfaceEntry 7 }


-- dma.2.2.1.4
stResources OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Server resources status."
   ::= { stServers 4 }


-- dma.2.2.1.4.1
stRsrcCPUUsageTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StRsrcCPUUsageEntry
   MAX-ACCESS  not-accessible
```

```
    STATUS       current
    DESCRIPTION "CPU usage information for the servers."
    ::= { stResources 1 }


-- dma.2.2.1.4.1.1
stRsrcCPUUsageEntry OBJECT-TYPE
    SYNTAX       StRsrcCPUUsageEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in stRsrcCPUUsageTable."
    INDEX        { stRsrcCPUUsageIndex }
    ::= { stRsrcCPUUsageTable 1 }


StRsrcCPUUsageEntry ::= SEQUENCE
{
    stRsrcCPUUsageIndex             Unsigned32,
    stRsrcCPUUsageHostName          DisplayString,
    stRsrcCPUUsageCPUUtilizationPct  Unsigned32
}


-- dma.2.2.1.4.1.1.1
stRsrcCPUUsageIndex OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "stRsrcCPUUsageTable index."
    ::= { stRsrcCPUUsageEntry 1 }


-- dma.2.2.1.4.1.1.2
stRsrcCPUUsageHostName OBJECT-TYPE
    SYNTAX       DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Hostname of the server."
    ::= { stRsrcCPUUsageEntry 2 }


-- dma.2.2.1.4.1.1.3
stRsrcCPUUsageCPUUtilizationPct OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "CPU utilization percentage of the server."
    ::= { stRsrcCPUUsageEntry 3 }


-- dma.2.2.1.4.2
stRsrcMemoryUsageTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF StRsrcMemoryUsageEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Memory usage information for the servers."
```

```
    ::= { stResources 2 }


-- dma.2.2.1.4.2.1
stRsrcMemoryUsageEntry OBJECT-TYPE
    SYNTAX      StRsrcMemoryUsageEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stRsrcMemoryUsageTable."
    INDEX       { stRsrcMemUsageIndex }
    ::= { stRsrcMemoryUsageTable 1 }


StRsrcMemoryUsageEntry ::= SEQUENCE
{
    stRsrcMemUsageIndex          Unsigned32,
    stRsrcMemUsageHostName       DisplayString,
    stRsrcMemUsageTotalMemory    Unsigned32,
    stRsrcMemUsageBuffersAndCache Unsigned32,
    stRsrcMemUsageUsed           Unsigned32,
    stRsrcMemUsageFree           Unsigned32
}

-- dma.2.2.1.4.2.1.1
stRsrcMemUsageIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stRsrcMemoryUsageTable index."
    ::= { stRsrcMemoryUsageEntry 1 }

-- dma.2.2.1.4.2.1.2
stRsrcMemUsageHostName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Hostname of the server."
    ::= { stRsrcMemoryUsageEntry 2 }

-- dma.2.2.1.4.2.1.3
stRsrcMemUsageTotalMemory OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Total system memory in the server (MB)."
    ::= { stRsrcMemoryUsageEntry 3 }

-- dma.2.2.1.4.2.1.4
stRsrcMemUsageBuffersAndCache OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION "System memory used for buffers and cache (MB)."
    ::= { stRsrcMemoryUsageEntry 4 }


-- dma.2.2.1.4.2.1.5
stRsrcMemUsageUsed OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "System memory used by processes (MB)."
    ::= { stRsrcMemoryUsageEntry 5 }


-- dma.2.2.1.4.2.1.6
stRsrcMemUsageFree OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "System memory unused (MB)."
    ::= { stRsrcMemoryUsageEntry 6 }


-- dma.2.2.1.4.3
stRsrcSwapSpaceTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF StRsrcSwapSpaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Swap space information for the servers."
    ::= { stResources 3 }


-- dma.2.2.1.4.3.1
stRsrcSwapSpaceEntry OBJECT-TYPE
    SYNTAX      StRsrcSwapSpaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stRsrcSwapSpaceTable"
    INDEX       { stRsrcSwapIndex }
    ::= { stRsrcSwapSpaceTable 1 }

StRsrcSwapSpaceEntry ::= SEQUENCE
{
    stRsrcSwapIndex      Unsigned32,
    stRsrcSwapHostName   DisplayString,
    stRsrcSwapTotal      Unsigned32,
    stRsrcSwapUsed       Unsigned32
}

-- dma.2.2.1.4.3.1.1
stRsrcSwapIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stRsrcSpaceTable index."
```

```
   ::= { stRsrcSwapSpaceEntry 1 }


-- dma.2.2.1.4.3.1.2
stRsrcSwapHostName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Hostname of the server."
   ::= { stRsrcSwapSpaceEntry 2 }


-- dma.2.2.1.4.3.1.3
stRsrcSwapTotal OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Total swap space allocated in the system (MB)."
   ::= { stRsrcSwapSpaceEntry 3 }


-- dma.2.2.1.4.3.1.4
stRsrcSwapUsed OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Swap space used by the system (MB)."
   ::= { stRsrcSwapSpaceEntry 4 }


-- dma.2.2.1.4.4
stRsrcDiskSpaceTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StRsrcDiskSpaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Disk space usage information for the servers."
   ::= { stResources 4 }


-- dma.2.2.1.4.4.1
stRsrcDiskSpaceEntry OBJECT-TYPE
   SYNTAX      StRsrcDiskSpaceEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stRsrcDiskSpaceTable."
   INDEX       { stRsrcDiskIndex }
   ::= { stRsrcDiskSpaceTable 1 }

StRsrcDiskSpaceEntry ::= SEQUENCE
{
   stRsrcDiskIndex       Unsigned32,
   stRsrcDiskHostName    DisplayString,
   stRsrcDiskTotal       Unsigned32,
   stRsrcDiskUsed        Unsigned32
}
```

```
-- dma.2.2.1.4.4.1.1
stRsrcDiskIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stRsrcDiskSpaceTable index."
    ::= { stRsrcDiskSpaceEntry 1 }


-- dma.2.2.1.4.4.1.2
stRsrcDiskHostName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Hostname of the server."
    ::= { stRsrcDiskSpaceEntry 2 }


-- dma.2.2.1.4.4.1.3
stRsrcDiskTotal OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Total disk space available for DMA usage (MB)."
    ::= { stRsrcDiskSpaceEntry 3 }


-- dma.2.2.1.4.4.1.4
stRsrcDiskUsed OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Disk space used by DMA (MB)."
    ::= { stRsrcDiskSpaceEntry 4 }


-- dma.2.2.1.4.5
stRsrcLogSpaceTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF StRsrcLogSpaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Log space usage information for the servers."
    ::= { stResources 5 }


-- dma.2.2.1.4.5.1
stRsrcLogSpaceEntry OBJECT-TYPE
    SYNTAX      StRsrcLogSpaceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stRsrcLogSpaceTable"
    INDEX       { stRsrcLogIndex }
    ::= { stRsrcLogSpaceTable 1 }
```

```
StRsrcLogSpaceEntry ::= SEQUENCE
{
    stRsrcLogIndex            Unsigned32,
    stRsrcLogHostName         DisplayString,
    stRsrcLogTotal            Unsigned32,
    stRsrcLogUsed             Unsigned32,
    stRsrcLogWarningThreshold Unsigned32,
    stRsrcLogNextPurge        DateAndTime
}

-- dma.2.2.1.4.5.1.1
stRsrcLogIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stRsrcLogSpaceTable index."
    ::= { stRsrcLogSpaceEntry 1 }

-- dma.2.2.1.4.5.1.2
stRsrcLogHostName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Hostname of the server."
    ::= { stRsrcLogSpaceEntry 2 }

-- dma.2.2.1.4.5.1.3
stRsrcLogTotal OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Total disk space allocated for log archive storage (MB)."
    ::= { stRsrcLogSpaceEntry 3 }

-- dma.2.2.1.4.5.1.4
stRsrcLogUsed OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Disk space used by log archives (MB)."
    ::= { stRsrcLogSpaceEntry 4 }

-- dma.2.2.1.4.5.1.5
stRsrcLogWarningThreshold OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Percentage of log archive capacity at which a system alert should be generated."
    ::= { stRsrcLogSpaceEntry 5 }
```

```
-- dma.2.2.1.4.5.1.6
stRsrcLogNextPurge OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Date at which log archives will be subject to purging, based on age and
                 configuration."
    ::= { stRsrcLogSpaceEntry 6 }


-- dma.2.2.2
stDevices OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Status of devices connecting to DMA systems."
    ::= { dmaStatus 2 }


-- dma.2.2.2.1
stMCUs OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Status of MCUs connecting to DMA systems."
    ::= { stDevices 1 }


-- dma.2.2.2.1.1
stMCUCount OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Number of indexed entries in the tables within stMCUs."
    ::= { stMCUs 1 }


-- dma.2.2.2.1.2
stMCUStatusTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF StMCUStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Basic status information about configured MCUs."
    ::= { stMCUs 2 }


-- dma.2.2.2.1.2.1
stMCUStatusEntry OBJECT-TYPE
    SYNTAX       StMCUStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in stMCUStatusTable."
    INDEX        { stMCUStIndex }
    ::= { stMCUStatusTable 1 }


StMCUStatusEntry ::= SEQUENCE
{
    stMCUStIndex                Unsigned32,
    stMCUStName                 GeneralString,
```

```
    stMCUStServiceStatus        INTEGER,
    stMCUStHasAlert             TruthValue,
    stMCUStRecordingAvailable   TruthValue,
    stMCUStIVRAvailable         TruthValue
}
```

-- dma.2.2.2.1.2.1.1
```
stMCUStIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stMCUStatusTable index."
    ::= { stMCUStatusEntry 1 }
```

-- dma.2.2.2.1.2.1.2
```
stMCUStName OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the MCU."
    ::= { stMCUStatusEntry 2 }
```

-- dma.2.2.2.1.2.1.3
```
stMCUStServiceStatus OBJECT-TYPE
    SYNTAX      INTEGER
                { inService(1), busyOut(2), outOfService(3) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Service status of the MCU."
    ::= { stMCUStatusEntry 3 }
```

-- dma.2.2.2.1.2.1.4
```
stMCUStHasAlert OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the MCU has an alert condition."
    ::= { stMCUStatusEntry 4 }
```

-- dma.2.2.2.1.2.1.5
```
stMCUStRecordingAvailable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the MCU can provide conference recording services."
    ::= { stMCUStatusEntry 5 }
```

-- dma.2.2.2.1.2.1.6
```
stMCUStIVRAvailable OBJECT-TYPE
    SYNTAX      TruthValue
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the MCU can provide IVR services."
    ::= { stMCUStatusEntry 6 }


-- dma.2.2.2.1.3
stMCUVideoPortUsageTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF StMCUVideoPortUsageEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Video port usage information for configured MCUs."
    ::= { stMCUs 3 }


-- dma.2.2.2.1.3.1
stMCUVideoPortUsageEntry OBJECT-TYPE
    SYNTAX      StMCUVideoPortUsageEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stMCUVideoPortUsageTable."
    INDEX       { stMCUVidUsageIndex }
    ::= { stMCUVideoPortUsageTable 1 }


StMCUVideoPortUsageEntry ::= SEQUENCE
{
    stMCUVidUsageIndex          Unsigned32,
    stMCUVidUsageName           GeneralString,
    stMCUVidUsageMCUTotal       Unsigned32,
    stMCUVidUsageMCUUsed        Unsigned32,
    stMCUVidUsageDMATotal       Unsigned32,
    stMCUVidUsageDMAUsed        Unsigned32,
    stMCUVidUsageCMAReserved    Unsigned32
}


-- dma.2.2.2.1.3.1.1
stMCUVidUsageIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stMCUVideoPortUsageTable index."
    ::= { stMCUVideoPortUsageEntry 1 }


-- dma.2.2.2.1.3.1.2
stMCUVidUsageName OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the MCU."
    ::= { stMCUVideoPortUsageEntry 2 }


-- dma.2.2.2.1.3.1.3
```

```
stMCUVidUsageMCUTotal OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Total video ports available on the MCU."
   ::= { stMCUVideoPortUsageEntry 3 }


-- dma.2.2.2.1.3.1.4
stMCUVidUsageMCUUsed OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Video ports in use on the MCU."
   ::= { stMCUVideoPortUsageEntry 4 }


-- dma.2.2.2.1.3.1.5
stMCUVidUsageDMATotal OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Total video ports on the MCU available to DMA."
   ::= { stMCUVideoPortUsageEntry 5 }


-- dma.2.2.2.1.3.1.6
stMCUVidUsageDMAUsed OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Video ports in use on the MCU by DMA."
   ::= { stMCUVideoPortUsageEntry 6 }


-- dma.2.2.2.1.3.1.7
stMCUVidUsageCMAReserved OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Video ports on the MCU reserved for CMA."
   ::= { stMCUVideoPortUsageEntry 7 }


-- dma.2.2.2.1.4
stMCUVoicePortUsageTable OBJECT-TYPE
   SYNTAX       SEQUENCE OF StMCUVoicePortUsageEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "Voice port usage information for configured MCUs."
   ::= { stMCUs 4 }


-- dma.2.2.2.1.4.1
stMCUVoicePortUsageEntry OBJECT-TYPE
   SYNTAX       StMCUVoicePortUsageEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stMCUVoicePortUsageTable."
    INDEX       { stMCUVoxUsageIndex }
    ::= { stMCUVoicePortUsageTable 1 }

StMCUVoicePortUsageEntry ::= SEQUENCE
{
    stMCUVoxUsageIndex      Unsigned32,
    stMCUVoxUsageName       GeneralString,
    stMCUVoxUsageMCUTotal   Unsigned32,
    stMCUVoxUsageMCUUsed    Unsigned32,
    stMCUVoxUsageDMATotal   Unsigned32,
    stMCUVoxUsageDMAUsed    Unsigned32
}

-- dma.2.2.2.1.4.1.1
stMCUVoxUsageIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "stMCUVoicePortUsageTable index."
    ::= { stMCUVoicePortUsageEntry 1 }

-- dma.2.2.2.1.4.1.2
stMCUVoxUsageName OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the MCU."
    ::= { stMCUVoicePortUsageEntry 2 }

-- dma.2.2.2.1.4.1.3
stMCUVoxUsageMCUTotal OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Total voice ports available on the MCU."
    ::= { stMCUVoicePortUsageEntry 3 }

-- dma.2.2.2.1.4.1.4
stMCUVoxUsageMCUUsed OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Voice ports in use on the MCU."
    ::= { stMCUVoicePortUsageEntry 4 }

-- dma.2.2.2.1.4.1.5
stMCUVoxUsageDMATotal OBJECT-TYPE
```

```
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Total voice ports on the MCU available to DMA."
    ::= { stMCUVoicePortUsageEntry 5 }


-- dma.2.2.2.1.4.1.6
stMCUVoxUsageDMAUsed OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Voice ports in use on the MCU by DMA."
    ::= { stMCUVoicePortUsageEntry 6 }


-- dma.2.2.2.2
stMCUsPerCluster OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Per-cluster status of MCUs connecting to the DMA."
    ::= { stDevices 2 }


-- dma.2.2.2.2.1
stMCUsPerClusterCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of indexed entries in the tables within stMCUsPerCluster."
    ::= { stMCUsPerCluster 1 }


-- dma.2.2.2.2.2
stMCUPCConnectionStatusTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF StMCUPCConnectionStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Connection status information for configured MCUs."
    ::= { stMCUsPerCluster 2 }


-- dma.2.2.2.2.2.1
stMCUPCConnectionStatusEntry OBJECT-TYPE
    SYNTAX      StMCUPCConnectionStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stMCUPCConnectionStatusTable"
    INDEX       { stMCUPCConnStIndex }
    ::= { stMCUPCConnectionStatusTable 1 }


StMCUPCConnectionStatusEntry ::= SEQUENCE
{
    stMCUPCConnStIndex              Unsigned32,
    stMCUPCConnStName               GeneralString,
    stMCUPCConnStClusterName        DisplayString,
```

```
    stMCUPCConnStConnectionStatus INTEGER
}

-- dma.2.2.2.2.2.1.1
stMCUPCConnStIndex OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stMCUPCConnectionStatusTable index."
   ::= { stMCUPCConnectionStatusEntry 1 }

-- dma.2.2.2.2.2.1.2
stMCUPCConnStName OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of the MCU."
   ::= { stMCUPCConnectionStatusEntry 2 }

-- dma.2.2.2.2.2.1.3
stMCUPCConnStClusterName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Cluster from which the MCU status is being observed."
   ::= { stMCUPCConnectionStatusEntry 3 }

-- dma.2.2.2.2.2.1.4
stMCUPCConnStConnectionStatus OBJECT-TYPE
   SYNTAX      INTEGER
               { notConfigured(1), notConnected(2), connected(3), connectedSecurely(4) }
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Status of the connection to the MCU."
   ::= { stMCUPCConnectionStatusEntry 4 }

-- dma.2.2.2.2.3
stMCUPCReliabilityStatsTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF StMCUPCReliabilityStatsEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Reliability statistics information for configured MCUs."
   ::= { stMCUsPerCluster 3 }

-- dma.2.2.2.2.3.1
stMCUPCReliabilityStatsEntry OBJECT-TYPE
   SYNTAX      StMCUPCReliabilityStatsEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "An entry in stMCUPCReliabilityStatsTable."
```

```
    INDEX        { stMCUPCRelIndex }
    ::= { stMCUPCReliabilityStatsTable 1 }

StMCUPCReliabilityStatsEntry ::= SEQUENCE
{
    stMCUPCRelIndex            Unsigned32,
    stMCUPCRelName             GeneralString,
    stMCUPCRelClusterName      DisplayString,
    stMCUPCRelDisconnects      Unsigned32,
    stMCUPCRelCallFailureRate  Unsigned32
}

-- dma.2.2.2.2.3.1.1
stMCUPCRelIndex OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "stMCUPCReliabilityStatsTable index."
    ::= { stMCUPCReliabilityStatsEntry 1 }

-- dma.2.2.2.2.3.1.2
stMCUPCRelName OBJECT-TYPE
    SYNTAX       GeneralString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "Name of the MCU."
    ::= { stMCUPCReliabilityStatsEntry 2 }

-- dma.2.2.2.2.3.1.3
stMCUPCRelClusterName OBJECT-TYPE
    SYNTAX       DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "Cluster from which the MCU status is being observed."
    ::= { stMCUPCReliabilityStatsEntry 3 }

-- dma.2.2.2.2.3.1.4
stMCUPCRelDisconnects OBJECT-TYPE
    SYNTAX       Unsigned32
    UNITS        "hundredths"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "Number of MCU disconnects observed by this cluster in the past 24 hours, divided
                 by the number of conference manager territories. This integer should be divided by
                 100 to get the intended value."
    ::= { stMCUPCReliabilityStatsEntry 4 }

-- dma.2.2.2.2.3.1.5
stMCUPCRelCallFailureRate OBJECT-TYPE
    SYNTAX       Unsigned32
```

```
        UNITS        "hundredths"
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION "Current call failure rate observed by this cluster. This integer should be
divided
                     by 100 to get the intended value."
        ::= { stMCUPCReliabilityStatsEntry 5 }

-- dma.2.2.3
stClusters OBJECT-IDENTITY
        STATUS       current
        DESCRIPTION "Information about clusters in the DMA supercluster."
        ::= { dmaStatus 3 }

-- dma.2.2.3.1
stClustersCount OBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION "Number of indexed entries in the tables within stClusters."
        ::= { stClusters 1 }

-- dma.2.2.3.2
stClustersTable OBJECT-TYPE
        SYNTAX       SEQUENCE OF StClustersEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION "Status of individual clusters in the supercluster."
        ::= { stClusters 2 }

-- dma.2.2.3.2.1
stClustersEntry OBJECT-TYPE
        SYNTAX       StClustersEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION "An entry in stClustersTable."
        INDEX        { stClIndex }
        ::= { stClustersTable 1 }

StClustersEntry ::= SEQUENCE
{
    stClIndex         Unsigned32,
    stClClusterName   DisplayString,
    stClClusterStatus INTEGER
}

-- dma.2.2.3.2.1.1
stClIndex OBJECT-TYPE
        SYNTAX       Unsigned32
        MAX-ACCESS   not-accessible
```

```
    STATUS      current
    DESCRIPTION "stClustersTable index."
    ::= { stClustersEntry 1 }


-- dma.2.2.3.2.1.2
stClClusterName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the cluster."
    ::= { stClustersEntry 2 }


-- dma.2.2.3.2.1.3
stClClusterStatus OBJECT-TYPE
    SYNTAX      INTEGER
                { inService(1), busyOut(2), outOfService(3) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Service status of the cluster."
    ::= { stClustersEntry 3 }


-- dma.2.2.3.3
stLicensesTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF StLicensesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Licensing status of clusters in the supercluster."
    ::= { stClusters 3 }


-- dma.2.2.3.3.1
stLicensesEntry OBJECT-TYPE
    SYNTAX      StLicensesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in stLicensesTable."
    INDEX       { stLicIndex }
    ::= { stLicensesTable 1 }



StLicensesEntry ::= SEQUENCE
{
    stLicIndex                Unsigned32,
    stLicClusterName          DisplayString,
    stLicLicenseStatus        INTEGER,
    stLicLicensedCalls        Unsigned32,
    stLicCallserverActiveCalls Unsigned32
}

-- dma.2.2.3.3.1.1
stLicIndex OBJECT-TYPE
```

```
   SYNTAX      Unsigned32
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "stLicensesTable index."
   ::= { stLicensesEntry 1 }


-- dma.2.2.3.3.1.2
stLicClusterName OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of the cluster."
   ::= { stLicensesEntry 2 }


-- dma.2.2.3.3.1.3
stLicLicenseStatus OBJECT-TYPE
   SYNTAX      INTEGER
               { valid(1), invalid(2), notInstalled(3) }
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "State of the cluster's license."
   ::= { stLicensesEntry 3 }


-- dma.2.2.3.3.1.4
stLicLicensedCalls OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Maximum number of concurrent calls afforded by the installed license."
   ::= { stLicensesEntry 4 }


-- dma.2.2.3.3.1.5
stLicCallserverActiveCalls OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of license slots used by the currently active calls."
   ::= { stLicensesEntry 5 }


-- dma.2.2.4
stCallserver OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Status of the DMA call server."
   ::= { dmaStatus 4 }


-- dma.2.2.4.1
stCsSupercluster OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Call server status shared across the supercluster."
   ::= { stCallserver 1 }
```

```
-- dma.2.2.4.1.1
stCsSiteTopology OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Supercluster-wide site topology status."
    ::= { stCsSupercluster 1 }


-- dma.2.2.4.1.1.1
stCsConfMgrTerritoriesCount OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Number of indexed entries in stCsConfMgrTerritoriesTable."
    ::= { stCsSiteTopology 1 }


-- dma.2.2.4.1.1.2
stCsConfMgrTerritoriesTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF StCsConfMgrTerritoriesEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Territories configured to host conference rooms."
    ::= { stCsSiteTopology 2 }


-- dma.2.2.4.1.1.2.1
stCsConfMgrTerritoriesEntry OBJECT-TYPE
    SYNTAX       StCsConfMgrTerritoriesEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in stCsConfMgrTerritoriesTable."
    INDEX        { stCsConfMgrTerrIndex }
    ::= { stCsConfMgrTerritoriesTable 1 }


StCsConfMgrTerritoriesEntry ::= SEQUENCE
{
    stCsConfMgrTerrIndex Unsigned32,
    stCsConfMgrTerrName  GeneralString
}

-- dma.2.2.4.1.1.2.1.1
stCsConfMgrTerrIndex OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "stCsConfMgrTerritoriesTable index."
    ::= { stCsConfMgrTerritoriesEntry 1 }


-- dma.2.2.4.1.1.2.1.2
stCsConfMgrTerrName OBJECT-TYPE
    SYNTAX       GeneralString
    MAX-ACCESS   read-only
```

```
    STATUS      current
    DESCRIPTION "Name of the territory."
    ::= { stCsConfMgrTerritoriesEntry 2 }


-- dma.2.2.4.1.2
stCsIntegrations OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for systems with which the DMA integrates."
    ::= { stCsSupercluster 2 }


-- dma.2.2.4.1.2.1
stCsIntDirectoryService OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for directory service integration."
    ::= { stCsIntegrations 1 }


-- dma.2.2.4.1.2.1.1
stCsIntDirSvcMSActiveDirectory OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for Microsoft Active Directory integration."
    ::= { stCsIntDirectoryService 1 }


-- dma.2.2.4.1.2.1.1.1
stCsIntMSADEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if Active Directory integration is enabled."
    ::= { stCsIntDirSvcMSActiveDirectory 1 }


-- dma.2.2.4.1.2.1.1.2
stCsIntMSADCacheStatus OBJECT-TYPE
    SYNTAX      INTEGER
                { disabled(1), connecting(2), integrated(3), integratedWithoutEncryption(4),
                failed(5), outdated(6), failedNoSuchEnterpriseUser(7),
                failedEnterpriseAuthentication(8), failedInvalidEnterpriseCredentials(9),
                failedEnterpriseAuthenticationWithCode(10), failedConnection(11) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Status of Active Directory caching."
    ::= { stCsIntDirSvcMSActiveDirectory 2 }


-- dma.2.2.4.1.2.1.1.3
stCsIntMSADCachingCluster OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of cluster performing AD caching."
    ::= { stCsIntDirSvcMSActiveDirectory 3 }
```

```
-- dma.2.2.4.1.2.1.1.4
stCsIntMSADCachingServer OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Name of server performing AD caching."
   ::= { stCsIntDirSvcMSActiveDirectory 4 }


-- dma.2.2.4.1.2.1.1.5
stCsIntMSADConnectionSecure OBJECT-TYPE
   SYNTAX      TruthValue
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "True if connection to AD is encrypted."
   ::= { stCsIntDirSvcMSActiveDirectory 5 }


-- dma.2.2.4.1.2.1.1.6
stCsIntMSADCacheRefreshDate OBJECT-TYPE
   SYNTAX      DateAndTime
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Time of last cache refresh."
   ::= { stCsIntDirSvcMSActiveDirectory 6 }


-- dma.2.2.4.1.2.1.1.7
stCsIntMSADEnterpriseConfRooms OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of enterprise conference rooms generated by AD integration."
   ::= { stCsIntDirSvcMSActiveDirectory 7 }


-- dma.2.2.4.1.2.2
stCsIntCalendaring OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Status for calendaring integration."
   ::= { stCsIntegrations 2 }


-- dma.2.2.4.1.2.2.1
stCsIntCalMSExchange OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Status for Microsoft Exchange integration."
   ::= { stCsIntCalendaring 1 }


-- dma.2.2.4.1.2.2.1.1
stCsIntMSExchEnabled OBJECT-TYPE
   SYNTAX      TruthValue
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "True if Exchange integration is enabled."
```

```
    ::= { stCsIntCalMSExchange 1 }


-- dma.2.2.4.1.2.2.1.2
stCsIntMSExchSubscriptionStatus OBJECT-TYPE
    SYNTAX      INTEGER
                { unknown(1), unavailable(2), error(3), disabled(4),
                ignoredNoEnterpriseDirectory(5), ignoredMailboxNotFound(6), authFailed(7),
                subscriptionPending(8), processingOk(9) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Status of Exchange mailbox subscription and processing."
    ::= { stCsIntCalMSExchange 2 }


-- dma.2.2.4.1.2.2.1.3
stCsIntMSExchIntegratingCluster OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of cluster performing Exchange integration."
    ::= { stCsIntCalMSExchange 3 }


-- dma.2.2.4.1.2.2.1.4
stCsIntMSExchIntegratingServer OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of server performing Exchange integration."
    ::= { stCsIntCalMSExchange 4 }


-- dma.2.2.4.1.2.2.1.5
stCsIntMSExchMailbox OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Detected SMTP email address for Exchange integration service account."
    ::= { stCsIntCalMSExchange 5 }


-- dma.2.2.4.1.2.2.1.6
stCsIntMSExchMeetingsToday OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of PCO-scheduled meetings scheduled for the current calendar day, per the
                service account's Exchange calendar."
    ::= { stCsIntCalMSExchange 6 }


-- dma.2.2.4.1.2.3
stCsIntSiteTopology OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for site topology service integration."
```

```
    ::= { stCsIntegrations 3 }


-- dma.2.2.4.1.2.3.1
stCsIntSiteTopoPolycomCMA OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for Polycom CMA system integration."
    ::= { stCsIntSiteTopology 1 }


-- dma.2.2.4.1.2.3.1.1
stCsIntPlcmCMAEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if CMA integration is enabled."
    ::= { stCsIntSiteTopoPolycomCMA 1 }


-- dma.2.2.4.1.2.3.1.2
stCsIntPlcmCMAConnectionStatus OBJECT-TYPE
    SYNTAX      INTEGER
                { connectionOk(1), connectionFailed(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Status of the connection to the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 2 }


-- dma.2.2.4.1.2.3.1.3
stCsIntPlcmCMALastContactDate OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Time of the DMA's last contact with the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 3 }


-- dma.2.2.4.1.2.3.1.4
stCsIntPlcmCMATimeSinceLastRefresh OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Time elapsed since the DMA last synchronized its data to that provided by the CMA
                system."
    ::= { stCsIntSiteTopoPolycomCMA 4 }


-- dma.2.2.4.1.2.3.1.5
stCsIntPlcmCMATerritories OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of territories provided by the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 5 }
```

```
-- dma.2.2.4.1.2.3.1.6
stCsIntPlcmCMASites OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of sites provided by the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 6 }


-- dma.2.2.4.1.2.3.1.7
stCsIntPlcmCMASiteLinks OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of site links provided by the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 7 }


-- dma.2.2.4.1.2.3.1.8
stCsIntPlcmCMAMPLSClouds OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of MPLS clouds provided by the CMA system."
    ::= { stCsIntSiteTopoPolycomCMA 8 }


-- dma.2.2.4.1.2.4
stCsIntNetwork OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for network integrations."
    ::= { stCsIntegrations 4 }


-- dma.2.2.4.1.2.4.1
stCsIntNetBandwidthManagement OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for bandwidth management integrations."
    ::= { stCsIntNetwork 1 }


-- dma.2.2.4.1.2.4.1.1
stCsIntNetBWMgmtJuniperSRC OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Status for Juniper Networks SRC integration."
    ::= { stCsIntNetBandwidthManagement 1 }


-- dma.2.2.4.1.2.4.1.1.1
stCsIntJuniperSRCEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if Juniper SRC integration is enabled."
    ::= { stCsIntNetBWMgmtJuniperSRC 1 }
```

```
-- dma.2.2.4.2
stCsDevices OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Status for devices connecting to the DMA call server."
   ::= { stCallserver 2 }


-- dma.2.2.4.2.1
stCsConfMgrMCUs OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Status for MCUs connecting to the DMA call server."
   ::= { stCsDevices 1 }


-- dma.2.2.4.2.1.1
stCsConfMgrMCUsCount OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Number of indexed entries in stCsConfMgrMCUsTables,"
   ::= { stCsConfMgrMCUs 1 }


-- dma.2.2.4.2.1.2
stCsConfMgrMCUsTable OBJECT-TYPE
   SYNTAX       SEQUENCE OF StCsConfMgrMCUsEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "MCUs configured as enabled for conference rooms."
   ::= { stCsConfMgrMCUs 2 }


-- dma.2.2.4.2.1.2.1
stCsConfMgrMCUsEntry OBJECT-TYPE
   SYNTAX       StCsConfMgrMCUsEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "An entry in stCsConfMgrMCUsTable"
   INDEX        { stCsCMMCUIndex }
   ::= { stCsConfMgrMCUsTable 1 }

StCsConfMgrMCUsEntry ::= SEQUENCE
{
   stCsCMMCUIndex Unsigned32,
   stCsCMMCUName  GeneralString
}

-- dma.2.2.4.2.1.2.1.1
stCsCMMCUIndex OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "stCsConfMgrMCUsTable index."
   ::= { stCsConfMgrMCUsEntry 1 }
```

```
-- dma.2.2.4.2.1.2.1.2
stCsCMMCUName OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the MCU."
    ::= { stCsConfMgrMCUsEntry 2 }


-- DMA USAGE


-- dma.2.3
dmaUsage OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains usage data for the DMA system."
    ::= { dmaMonitoring1 3 }


-- dma.2.3.1
useConfHistory OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains conference history data."
    ::= { dmaUsage 1 }


-- dma.2.3.1.1
useConfHistoryMaximumParticipants OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains historical data regarding maximum concurrent conference participant
                counts."
    ::= { useConfHistory 1 }


-- dma.2.3.1.1.1
useCHMaxPartsLast60MinutesCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of indexed entries in useCHMaxPartsLast60MinutesTable."
    ::= { useConfHistoryMaximumParticipants 1 }


-- dma.2.3.1.1.2
useCHMaxPartsLast60MinutesTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF UseCHMaxPartsLast60MinutesEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "Maximum concurrent conference participant counts for the past hour, taken at
                one-minute intervals."
    ::= { useConfHistoryMaximumParticipants 2 }


-- dma.2.3.1.1.2.1
useCHMaxPartsLast60MinutesEntry OBJECT-TYPE
    SYNTAX      UseCHMaxPartsLast60MinutesEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in useCHMaxPartsLast60MinutesTable."
    INDEX       { useCHMaxParts60MinIndex }
    ::= { useCHMaxPartsLast60MinutesTable 1 }

UseCHMaxPartsLast60MinutesEntry ::= SEQUENCE
{
    useCHMaxParts60MinIndex              Unsigned32,
    useCHMaxParts60MinClusterName        DisplayString,
    useCHMaxParts60MinTimestamp          DateAndTime,
    useCHMaxParts60MinMaxSimultaneousCalls Unsigned32,
    useCHMaxParts60MinMaxAdHocCalls      Unsigned32,
    useCHMaxParts60MinMaxPCOCalls        Unsigned32
}

-- dma.2.3.1.1.2.1.1
useCHMaxParts60MinIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "useCHMaxPartsLast60MinutesTable index."
    ::= { useCHMaxPartsLast60MinutesEntry 1 }

-- dma.2.3.1.1.2.1.2
useCHMaxParts60MinClusterName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Cluster in which the participant count entry was recorded."
    ::= { useCHMaxPartsLast60MinutesEntry 2 }

-- dma.2.3.1.1.2.1.3
useCHMaxParts60MinTimestamp OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Time at which the participant count entry was recorded."
    ::= { useCHMaxPartsLast60MinutesEntry 3 }

-- dma.2.3.1.1.2.1.4
useCHMaxParts60MinMaxSimultaneousCalls OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Maximum number of concurrent calls recorded on the cluster during the specified
                one-minute interval."
    ::= { useCHMaxPartsLast60MinutesEntry 4 }

-- dma.2.3.1.1.2.1.5
```

```
useCHMaxParts60MinMaxAdHocCalls OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Maxmimum number of concurrent ad-hoc calls recorded on the cluster during the
                specified one-minute interval."
    ::= { useCHMaxPartsLast60MinutesEntry 5 }


-- dma.2.3.1.1.2.1.6
useCHMaxParts60MinMaxPCOCalls OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Maximum number of concurrent calls to PCO-scheduled conference rooms recorded on
                the cluster during the specified one-minute interval."
    ::= { useCHMaxPartsLast60MinutesEntry 6 }


-- dma.2.3.1.1.3
useCHMaxPartsLast24HoursCount OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Number of indexed entries in useCHMaxPartsLast24HoursTable."
    ::= { useConfHistoryMaximumParticipants 3 }


-- dma.2.3.1.1.4
useCHMaxPartsLast24HoursTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF UseCHMaxPartsLast24HoursEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Maximum concurrent conference participant counts for the past day, taken at
                one-hour intervals."
    ::= { useConfHistoryMaximumParticipants 4 }


-- dma.2.3.1.1.4.1
useCHMaxPartsLast24HoursEntry OBJECT-TYPE
    SYNTAX       UseCHMaxPartsLast24HoursEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in useCHMaxPartsLast24HoursTable."
    INDEX        { useCHMaxParts24HrIndex }
    ::= { useCHMaxPartsLast24HoursTable 1 }


UseCHMaxPartsLast24HoursEntry ::= SEQUENCE
{
    useCHMaxParts24HrIndex                Unsigned32,
    useCHMaxParts24HrClusterName          DisplayString,
    useCHMaxParts24HrTimestamp            DateAndTime,
    useCHMaxParts24HrMaxSimultaneousCalls Unsigned32,
    useCHMaxParts24HrMaxAdHocCalls        Unsigned32,
```

```
    useCHMaxParts24HrMaxPCOCalls            Unsigned32
}
```

-- dma.2.3.1.1.4.1.1
useCHMaxParts24HrIndex OBJECT-TYPE
    SYNTAX   Unsigned32
    MAX-ACCESS not-accessible
    STATUS   current
    DESCRIPTION "useCHMaxPartsLast24HoursTable index."
    ::= { useCHMaxPartsLast24HoursEntry 1 }

-- dma.2.3.1.1.4.1.2
useCHMaxParts24HrClusterName OBJECT-TYPE
    SYNTAX   DisplayString
    MAX-ACCESS read-only
    STATUS   current
    DESCRIPTION "Cluster in which the participant count entry was recorded."
    ::= { useCHMaxPartsLast24HoursEntry 2 }

-- dma.2.3.1.1.4.1.3
useCHMaxParts24HrTimestamp OBJECT-TYPE
    SYNTAX   DateAndTime
    MAX-ACCESS read-only
    STATUS   current
    DESCRIPTION "Time at which the participant count entry was recorded."
    ::= { useCHMaxPartsLast24HoursEntry 3 }

-- dma.2.3.1.1.4.1.4
useCHMaxParts24HrMaxSimultaneousCalls OBJECT-TYPE
    SYNTAX   Unsigned32
    MAX-ACCESS read-only
    STATUS   current
    DESCRIPTION "Maximum number of concurrent calls recorded on the cluster during the specified
                one-hour interval."
    ::= { useCHMaxPartsLast24HoursEntry 4 }

-- dma.2.3.1.1.4.1.5
useCHMaxParts24HrMaxAdHocCalls OBJECT-TYPE
    SYNTAX   Unsigned32
    MAX-ACCESS read-only
    STATUS   current
    DESCRIPTION "Maximum number of concurrent ad-hoc calls recorded on the cluster during the
                specified one-hour interval."
    ::= { useCHMaxPartsLast24HoursEntry 5 }

-- dma.2.3.1.1.4.1.6
useCHMaxParts24HrMaxPCOCalls OBJECT-TYPE
    SYNTAX   Unsigned32
    MAX-ACCESS read-only
    STATUS   current
```

```
             DESCRIPTION "Maximum number of concurrent calls to PCO-scheduled conference rooms recorded on
                         the cluster during the specified one-hour interval."
             ::= { useCHMaxPartsLast24HoursEntry 6 }


-- dma.2.3.1.1.5
useCHMaxPartsLast180DaysCount OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Number of indexed entries in useCHMaxPartsLast180DaysTable."
    ::= { useConfHistoryMaximumParticipants 5 }


-- dma.2.3.1.1.6
useCHMaxPartsLast180DaysTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF UseCHMaxPartsLast180DaysEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Maximum concurrent conference participant counts for the past 180 days, taken at
                 one-day intervals."
    ::= { useConfHistoryMaximumParticipants 6 }


-- dma.2.3.1.1.6.1
useCHMaxPartsLast180DaysEntry OBJECT-TYPE
    SYNTAX       UseCHMaxPartsLast180DaysEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in useCHMaxPartsLast180DaysTable."
    INDEX        { useCHMaxParts180DaysIndex }
    ::= { useCHMaxPartsLast180DaysTable 1 }


UseCHMaxPartsLast180DaysEntry ::= SEQUENCE
{
    useCHMaxParts180DaysIndex                Unsigned32,
    useCHMaxParts180DaysClusterName          DisplayString,
    useCHMaxParts180DaysTimestamp            DateAndTime,
    useCHMaxParts180DaysMaxSimultaneousCalls Unsigned32,
    useCHMaxParts180DaysMaxAdHocCalls        Unsigned32,
    useCHMaxParts180DaysMaxPCOCalls          Unsigned32
}


-- dma.2.3.1.1.6.1.1
useCHMaxParts180DaysIndex OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "useCHMaxPartsLast180DaysTable index."
    ::= { useCHMaxPartsLast180DaysEntry 1 }


-- dma.2.3.1.1.6.1.2
useCHMaxParts180DaysClusterName OBJECT-TYPE
```

```
   SYNTAX      DisplayString
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Cluster in which the participant count entry was recorded."
   ::= { useCHMaxPartsLast180DaysEntry 2 }


-- dma.2.3.1.1.6.1.3
useCHMaxParts180DaysTimestamp OBJECT-TYPE
   SYNTAX      DateAndTime
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Time at which the participant count entry was recorded."
   ::= { useCHMaxPartsLast180DaysEntry 3 }


-- dma.2.3.1.1.6.1.4
useCHMaxParts180DaysMaxSimultaneousCalls OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Maximum number of concurrent calls recorded on the cluster during the specified
               one-day interval."
   ::= { useCHMaxPartsLast180DaysEntry 4 }


-- dma.2.3.1.1.6.1.5
useCHMaxParts180DaysMaxAdHocCalls OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Maximum number of concurrent ad-hoc calls recorded on the cluster during the
               specified one-day interval."
   ::= { useCHMaxPartsLast180DaysEntry 5 }


-- dma.2.3.1.1.6.1.6
useCHMaxParts180DaysMaxPCOCalls OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Maximum number of concurrent calls to PCO-scheduled conference rooms recorded on
               the cluster during the specified one-minute interval."
   ::= { useCHMaxPartsLast180DaysEntry 6 }


-- dma.2.3.2
useCurrentConferences OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Contains current conferences usage data."
   ::= { dmaUsage 2 }


-- dma.2.3.2.1
useCurrentConfsConfManagerUsage OBJECT-IDENTITY
   STATUS      current
```

```
    DESCRIPTION "Contains usage data for the conference manager feature of DMA."
    ::= { useCurrentConferences 1 }


-- dma.2.3.2.1.1
useConfMgrUsageCount OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "Number of indexed entries in useConfMgrUsageTable."
    ::= { useCurrentConfsConfManagerUsage 1 }


-- dma.2.3.2.1.2
useConfMgrUsageTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF UseConfMgrUsageEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "Usage information (conferences, calls, etc.) for the DMA conference manager."
    ::= { useCurrentConfsConfManagerUsage 2 }


-- dma.2.3.2.1.2.1
useConfMgrUsageEntry OBJECT-TYPE
    SYNTAX       UseConfMgrUsageEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "An entry in useConfMgrUsageTable."
    INDEX        { useCMUsageIndex }
    ::= { useConfMgrUsageTable 1 }


UseConfMgrUsageEntry ::= SEQUENCE
{
    useCMUsageIndex           Unsigned32,
    useCMUsageClusterName     DisplayString,
    useCMUsageActiveConfs     Unsigned32,
    useCMUsageActiveParts     Unsigned32,
    useCMUsageTotalVideoPorts Unsigned32,
    useCMUsageUsedVideoPorts  Unsigned32,
    useCMUsageTotalVoicePorts Unsigned32,
    useCMUsageUsedVoicePorts  Unsigned32,
    useCMUsageLocalUsers      Unsigned32,
    useCMUsageCustomConfRooms Unsigned32
}

-- dma.2.3.2.1.2.1.1
useCMUsageIndex OBJECT-TYPE
    SYNTAX       Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "useConfMgrUsageTable index."
    ::= { useConfMgrUsageEntry 1 }
```

```
-- dma.2.3.2.1.2.1.2
useCMUsageClusterName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the cluster in which the usage data was recorded."
    ::= { useConfMgrUsageEntry 2 }


-- dma.2.3.2.1.2.1.3
useCMUsageActiveConfs OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of active conferences being serviced by the cluster."
    ::= { useConfMgrUsageEntry 3 }


-- dma.2.3.2.1.2.1.4
useCMUsageActiveParts OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of active conference participants being serviced by the cluster."
    ::= { useConfMgrUsageEntry 4 }


-- dma.2.3.2.1.2.1.5
useCMUsageTotalVideoPorts OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of video ports available to the cluster."
    ::= { useConfMgrUsageEntry 5 }


-- dma.2.3.2.1.2.1.6
useCMUsageUsedVideoPorts OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of video ports used in the cluster."
    ::= { useConfMgrUsageEntry 6 }


-- dma.2.3.2.1.2.1.7
useCMUsageTotalVoicePorts OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of voice ports available to the cluster."
    ::= { useConfMgrUsageEntry 7 }


-- dma.2.3.2.1.2.1.8
useCMUsageUsedVoicePorts OBJECT-TYPE
```

```
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of voice ports used in the cluster."
   ::= { useConfMgrUsageEntry 8 }


-- dma.2.3.2.1.2.1.9
useCMUsageLocalUsers OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of local users in the cluster's database."
   ::= { useConfMgrUsageEntry 9 }


-- dma.2.3.2.1.2.1.10
useCMUsageCustomConfRooms OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of custom conference rooms in the cluster's database."
   ::= { useConfMgrUsageEntry 10 }


-- dma.2.3.3
useDevices OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Contains device-related usage data."
   ::= { dmaUsage 3 }


-- dma.2.3.3.1
useDevRegistrations OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Contains information about devices currently registered to the DMA."
   ::= { useDevices 1 }


-- dma.2.3.3.1.1
useDevRegistrationsCount OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Number of indexed entries in useDevRegistrationsTable."
   ::= { useDevRegistrations 1 }


-- dma.2.3.3.1.2
useDevRegistrationsTable OBJECT-TYPE
   SYNTAX      SEQUENCE OF UseDevRegistrationsEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION "Device registrations per cluster."
   ::= { useDevRegistrations 2 }
```

```
-- dma.2.3.3.1.2.1
useDevRegistrationsEntry OBJECT-TYPE
    SYNTAX      UseDevRegistrationsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry in useDevRegistrationsTable."
    INDEX       { useDevRegIndex }
    ::= { useDevRegistrationsTable 1 }

UseDevRegistrationsEntry ::= SEQUENCE
{
    useDevRegIndex                       Unsigned32,
    useDevRegClusterName                 DisplayString,
    useDevRegActiveEndpointReg           Unsigned32,
    useDevRegInactiveEndpointReg         Unsigned32,
    useDevRegFailedEndpointRegLast24Hours  Unsigned32
}

-- dma.2.3.3.1.2.1.1
useDevRegIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "useDevRegistrationsTable index."
    ::= { useDevRegistrationsEntry 1 }

-- dma.2.3.3.1.2.1.2
useDevRegClusterName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Name of the cluster in which the usage data was recorded."
    ::= { useDevRegistrationsEntry 2 }

-- dma.2.3.3.1.2.1.3
useDevRegActiveEndpointReg OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of endpoints with an active registration status."
    ::= { useDevRegistrationsEntry 3 }

-- dma.2.3.3.1.2.1.4
useDevRegInactiveEndpointReg OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Number of endpoints with an inactive registration status."
    ::= { useDevRegistrationsEntry 4 }
```

```
-- dma.2.3.3.1.2.1.5
useDevRegFailedEndpointRegLast24Hours OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Number of registration attempts that resulted in failure over the last 24 hours,
as
               determined by retained registration history."
   ::= { useDevRegistrationsEntry 5 }


-- DMA ALERTS


-- dma.2.4
dmaAlerts OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Contains alert data for the DMA system."
   ::= { dmaMonitoring1 4 }


-- dma.2.4.1
alActiveAlerts OBJECT-IDENTITY
   STATUS       current
   DESCRIPTION "Contains alerts currently active on the DMA system."
   ::= { dmaAlerts 1 }


-- dma.2.4.1.1
alActiveAlertsCount OBJECT-TYPE
   SYNTAX       Unsigned32
   MAX-ACCESS   read-only
   STATUS       current
   DESCRIPTION "Number of indexed entries (active alerts) in alActiveAlertsTable."
   ::= { alActiveAlerts 1 }


-- dma.2.4.1.2
alActiveAlertsTable OBJECT-TYPE
   SYNTAX       SEQUENCE OF AlActiveAlertsEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "Alerts currently active on the DMA system."
   ::= { alActiveAlerts 2 }


-- dma.2.4.1.2.1
alActiveAlertsEntry OBJECT-TYPE
   SYNTAX       AlActiveAlertsEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION "An entry in alActiveAlertsTable"
   INDEX        { alActAlertIndex }
   ::= { alActiveAlertsTable 1 }


AlActiveAlertsEntry ::= SEQUENCE
```

```
{
    alActAlertIndex         Unsigned32,
    alActAlertID            GeneralString,
    alActAlertTimestamp     DateAndTime,
    alActAlertCode          Unsigned32,
    alActAlertSeverity      INTEGER,
    alActAlertDescription   OCTET STRING
}

-- dma.2.4.1.2.1.1
alActAlertIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "alActiveAlertsTable index."
    ::= { alActiveAlertsEntry 1 }


-- dma.2.4.1.2.1.2
alActAlertID OBJECT-TYPE
    SYNTAX      GeneralString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Internal identifier for the alert."
    ::= { alActiveAlertsEntry 2 }


-- dma.2.4.1.2.1.3
alActAlertTimestamp OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Time the alert was generated."
    ::= { alActiveAlertsEntry 3 }


-- dma.2.4.1.2.1.4
alActAlertCode OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Code of the alert."
    ::= { alActiveAlertsEntry 4 }


-- dma.2.4.1.2.1.5
alActAlertSeverity OBJECT-TYPE
    SYNTAX      INTEGER
                { warn(1), severe(2), critical(3) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Severity of the alert."
    ::= { alActiveAlertsEntry 5 }
```

```
-- dma.2.4.1.2.1.6
alActAlertDescription OBJECT-TYPE
   SYNTAX      OCTET STRING
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION "Text of the alert message."
   ::= { alActiveAlertsEntry 6 }


-- DMA NOTIFICATIONS

-- dma.2.5
dmaNotifications OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "DMA alert notifications."
   ::= { dmaMonitoring1 5 }


-- dma.2.5.1
ntfObjects OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Objects that will be included in alert notifications."
   ::= { dmaNotifications 1 }


-- dma.2.5.1.1
ntfObjAlertID OBJECT-TYPE
   SYNTAX      GeneralString
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION "Internal identifier for the alert."
   ::= { ntfObjects 1 }


-- dma.2.5.1.2
ntfObjAlertTimestamp OBJECT-TYPE
   SYNTAX      DateAndTime
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION "Time the alert was generated."
   ::= { ntfObjects 2 }


-- dma.2.5.1.3
ntfObjAlertCode OBJECT-TYPE
   SYNTAX      Unsigned32
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION "Code of the alert."
   ::= { ntfObjects 3 }


-- dma.2.5.1.4
ntfObjAlertSeverity OBJECT-TYPE
   SYNTAX      INTEGER
               { warn(1), severe(2), critical(3) }
```

```
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION "Severity of the alert."
   ::= { ntfObjects 4 }

-- dma.2.5.1.5
ntfObjAlertDescription OBJECT-TYPE
   SYNTAX      OCTET STRING
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION "Text of the alert message."
   ::= { ntfObjects 5 }

-- dma.2.5.2
ntfAlertNotifications OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Contains alert notification objects."
   ::= { dmaNotifications 2 }

-- dma.2.5.2.0
ntfAlertNotificationObjects OBJECT-IDENTITY
   STATUS      current
   DESCRIPTION "Alert notification objects."
   ::= { ntfAlertNotifications 0 }

-- dma.2.5.2.0.1001
ntfAlertClusterBusyOut NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster is in the busied-out state."
   ::= { ntfAlertNotificationObjects 1001 }

-- dma.2.5.2.0.1002
ntfAlertClusterOutOfService NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
```

```
   DESCRIPTION "A cluster is in the out-of-service state."
   ::= { ntfAlertNotificationObjects 1002 }

-- dma.2.5.2.0.1003
ntfAlertClusterOrphan NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster's replication link is no longer valid."
   ::= { ntfAlertNotificationObjects 1003 }

-- dma.2.5.2.0.1004
ntfAlertClusterUnreachable NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster is not communicating with the supercluster."
   ::= { ntfAlertNotificationObjects 1004 }

-- dma.2.5.2.0.1005
ntfAlertClusterPendingReplication NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster has inconsistencies between its server's (or servers') data and the
               supercluster's data."
   ::= { ntfAlertNotificationObjects 1005 }

-- dma.2.5.2.0.1101
ntfAlertTerritoryNotActiveBothClustersNotInService NOTIFICATION-TYPE
   OBJECTS
   {
```

```
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "A territory with both a primary and backup cluster configured is inactive because
                  neither cluster is in a viable state."
    ::= { ntfAlertNotificationObjects 1101 }

-- dma.2.5.2.0.1102
ntfAlertTerritoryNotActiveClusterNotInService NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "A territory with only a primary cluster configured is inactive because that
cluster
                  is not in a viable state."
    ::= { ntfAlertNotificationObjects 1102 }

-- dma.2.5.2.0.1103
ntfAlertTerritoryNoClustersAssigned NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "A territory is inactive because it no cluster(s) assigned to service it."
    ::= { ntfAlertNotificationObjects 1103 }

-- dma.2.5.2.0.1104
ntfAlertTerritoryPrimaryClusterNotInService NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
```

```
   }
   STATUS      current
   DESCRIPTION "A territory with a primary and backup cluster configured is currently running on
               its backup cluster."
   ::= { ntfAlertNotificationObjects 1104 }


-- dma.2.5.2.0.2001
ntfAlertCMAUser NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "An error occurred while attempting to synchronize data to the Polycom CMA
system."
   ::= { ntfAlertNotificationObjects 2001 }


-- dma.2.5.2.0.2002
ntfAlertCMAUnreachable NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The responsible DMA cluster is unable to communicate with the Polycom CMA
system."
   ::= { ntfAlertNotificationObjects 2002 }


-- dma.2.5.2.0.2101
ntfAlertEntDirIntegrationFailed NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The DMA system's cache of user and group data could not be updated from the
               Active Directory server."
   ::= { ntfAlertNotificationObjects 2101 }
```

```
-- dma.2.5.2.0.2102
ntfAlertEntDirNoConfRooms NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "After successfully updating user and group data from the Active Directory server,
                no conference rooms were generated."
   ::= { ntfAlertNotificationObjects 2102 }


-- dma.2.5.2.0.2103
ntfAlertEntDirPrimaryClusterNotInService NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The primary cluster for the territory configured for Active Directory integration
                is not in a viable state; the backup cluster is active but does not assume
                responsibility for updating the user and group data cache."
   ::= { ntfAlertNotificationObjects 2103 }


-- dma.2.5.2.0.2104
ntfAlertEntDirNotAvailable NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The user and group data cache cannot be updated from the Active Directory server
                because both the primary and backup clusters for the responsible territory are not
                in a viable state."
   ::= { ntfAlertNotificationObjects 2104 }


-- dma.2.5.2.0.2105
ntfAlertEntDirNotAvailableNoBackup NOTIFICATION-TYPE
```

```
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS        current
   DESCRIPTION "The user and group data cache cannot be updated from the Active Directory server
                because the primary cluster for the responsible territory is not in a viable state
                and no backup cluster is configured."
   ::= { ntfAlertNotificationObjects 2105 }

-- dma.2.5.2.0.2106
ntfAlertEntDirUserAuthConnectionFailed NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS        current
   DESCRIPTION "A cluster was unable to connect to the Active Directory for the purpose of
                authenticating a user's credentials."
   ::= { ntfAlertNotificationObjects 2106 }

-- dma.2.5.2.0.2107
ntfAlertEntDirCachingConnectionFailed NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS        current
   DESCRIPTION "The cluster responsible for updating the user and groups data cache was unable to
                communicate with the Active Directory server."
   ::= { ntfAlertNotificationObjects 2107 }

-- dma.2.5.2.0.2201
ntfAlertExchangePrimaryClusterNotInServiceBackupAvailable NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
```

516   Polycom, Inc.

```
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The primary cluster servicing the territory responsible for Exchange integration
is
              not in a viable state; the backup cluster is currently assuming this duty."
   ::= { ntfAlertNotificationObjects 2201 }

-- dma.2.5.2.0.2202
ntfAlertExchangeBothClustersNotInService NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "Both the primary and backup cluster configured for the territory responsible for
              Exchange integration are not in a viable state."
   ::= { ntfAlertNotificationObjects 2202 }

-- dma.2.5.2.0.2203
ntfAlertExchangePrimaryClusterNotInService NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The primary cluster servicing the territory responsible for Exchange integration
is
              not in a viable state; no backup cluster is configured."
   ::= { ntfAlertNotificationObjects 2203 }

-- dma.2.5.2.0.3001
ntfAlertSignalingNotEnabled NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
```

```
   }
   STATUS      current
   DESCRIPTION "No signaling interface is enabled for the cluster; calls to the cluster cannot be
               processed."
   ::= { ntfAlertNotificationObjects 3001 }

-- dma.2.5.2.0.3101
ntfAlertCertExpired NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's server certificate has expired."
   ::= { ntfAlertNotificationObjects 3101 }

-- dma.2.5.2.0.3102
ntfAlertCertExpireNow NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's server certificate will expire within 1 day."
   ::= { ntfAlertNotificationObjects 3102 }

-- dma.2.5.2.0.3103
ntfAlertCertExpireSoon NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's server certificate will expire soon (30 days or less)."
   ::= { ntfAlertNotificationObjects 3103 }

-- dma.2.5.2.0.3104
ntfAlertCertSecExpired NOTIFICATION-TYPE
```

```
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "One or more CA certificates on the cluster has expired."
   ::= { ntfAlertNotificationObjects 3104 }

-- dma.2.5.2.0.3105
ntfAlertCertSecExpireSoon NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "One or more CA certificates on the cluster will expire soon (30 days or less)."
   ::= { ntfAlertNotificationObjects 3105 }

-- dma.2.5.2.0.3201
ntfAlertLicenseNoKeys NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "No license key is installed on the cluster."
   ::= { ntfAlertNotificationObjects 3201 }

-- dma.2.5.2.0.3202
ntfAlertLicenseInvalidKeys NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
```

```
   STATUS      current
   DESCRIPTION "An invalid license key is installed on the cluster."
   ::= { ntfAlertNotificationObjects 3202 }


-- dma.2.5.2.0.3301
ntfAlertNetworkSingleNodeDetected NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster is configured to have two servers, but communication between the two
               servers is not working."
   ::= { ntfAlertNotificationObjects 3301 }


-- dma.2.5.2.0.3302
ntfAlertNetworkPrivateActive NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A cluster is configured to have one server, but the private network interface is
               enabled and active."
   ::= { ntfAlertNotificationObjects 3302 }


-- dma.2.5.2.0.3303
ntfAlertNetworkPrivateError NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The private network interface has a problem."
   ::= { ntfAlertNotificationObjects 3303 }


-- dma.2.5.2.0.3304
ntfAlertNetworkPublicError NOTIFICATION-TYPE
```

```
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "The public management (or combined) network interface has a problem."
    ::= { ntfAlertNotificationObjects 3304 }

-- dma.2.5.2.0.3305
ntfAlertNetworkSignalingError NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "The signaling network interface has a problem."
    ::= { ntfAlertNotificationObjects 3305 }

-- dma.2.5.2.0.3401
ntfAlertResourceDiskSpace NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "The disk space used by DMA is at 85% or more of capacity."
    ::= { ntfAlertNotificationObjects 3401 }

-- dma.2.5.2.0.3402
ntfAlertResourceLogsPurge NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
```

```
   STATUS      current
   DESCRIPTION "The age of older log archives on the server is approaching the configured
retention
               period and will be subject to purging."
   ::= { ntfAlertNotificationObjects 3402 }

-- dma.2.5.2.0.3403
ntfAlertResourceLogsExceedLimit NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The size of the log archives on the server is greater than the allocated 1 GB
               capacity; older logs will be deleted to return to a disk space usage within
               capacity."
   ::= { ntfAlertNotificationObjects 3403 }

-- dma.2.5.2.0.3404
ntfAlertResourceLogsNearLimit NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The size of the log archives on the server is greater than the configured warning
               threshold of allocated capacity."
   ::= { ntfAlertNotificationObjects 3404 }

-- dma.2.5.2.0.3405
ntfAlertResourceCPUOver50Percent NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The server's CPU usage is unusually high."
   ::= { ntfAlertNotificationObjects 3405 }
```

```
-- dma.2.5.2.0.3406
ntfAlertResourceCPUOver75Percent NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The server's CPU usage is exceptionally high."
    ::= { ntfAlertNotificationObjects 3406 }

-- dma.2.5.2.0.3501
ntfAlertAVVirusDetected NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The most recent system scan of the server detected malware."
    ::= { ntfAlertNotificationObjects 3501 }

-- dma.2.5.2.0.3502
ntfAlertAVUnsuccessful NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
        ntfObjAlertSeverity,
        ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The most recent system scan of the server did not complete successfully."
    ::= { ntfAlertNotificationObjects 3502 }

-- dma.2.5.2.0.3503
ntfAlertAVNeverSucceeded NOTIFICATION-TYPE
    OBJECTS
    {
        ntfObjAlertID,
        ntfObjAlertTimestamp,
        ntfObjAlertCode,
```

```
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The server has never completed a full system scan."
    ::= { ntfAlertNotificationObjects 3503 }


-- dma.2.5.2.0.3601
ntfAlertDataSyncVersion NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The cluster contains servers running different versions of the DMA software."
    ::= { ntfAlertNotificationObjects 3601 }


-- dma.2.5.2.0.3602
ntfAlertDataSyncSystemTime NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "There is a discrepancy of more than 10 seconds between the system times on the
                cluster's servers."
    ::= { ntfAlertNotificationObjects 3602 }


-- dma.2.5.2.0.3603
ntfAlertDataSyncADIntegration NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "The cluster's servers observe different statuses for Active Directory
integration."
    ::= { ntfAlertNotificationObjects 3603 }
```

```
-- dma.2.5.2.0.3604
ntfAlertDataSyncADConfRooms NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's servers have different counts of enterprise conference rooms."
   ::= { ntfAlertNotificationObjects 3604 }

-- dma.2.5.2.0.3605
ntfAlertDataSyncCustomConfRooms NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's servers have different counts of custom conference rooms."
   ::= { ntfAlertNotificationObjects 3605 }

-- dma.2.5.2.0.3606
ntfAlertDataSyncLocalUsers NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "The cluster's servers have non-identical sets of local users."
   ::= { ntfAlertNotificationObjects 3606 }

-- dma.2.5.2.0.4001
ntfAlertMCUBusyOut NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
```

```
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "An MCU is in the busied-out state."
   ::= { ntfAlertNotificationObjects 4001 }

-- dma.2.5.2.0.4002
ntfAlertMCUOutOfService NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "An MCU is in the out-of-service state."
   ::= { ntfAlertNotificationObjects 4002 }

-- dma.2.5.2.0.4003
ntfAlertMCUMultipleWarnings NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "An MCU has one or more warnings present."
   ::= { ntfAlertNotificationObjects 4003 }

-- dma.2.5.2.0.5001
ntfAlertITPSystemConfigurationError NOTIFICATION-TYPE
   OBJECTS
   {
      ntfObjAlertID,
      ntfObjAlertTimestamp,
      ntfObjAlertCode,
      ntfObjAlertSeverity,
      ntfObjAlertDescription
   }
   STATUS      current
   DESCRIPTION "A device identifying itself as an ITP system has registered to the call server
with
                invalid or incomplete configuration data."
   ::= { ntfAlertNotificationObjects 5001 }
```

```
-- dma.2.5.2.0.5002
ntfAlertEndpointSignalingAlert NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "One or more endpoints are sending excessive signaling traffic and have been
temporarily blacklisted
    and may have been quarantined."
    ::= { ntfAlertNotificationObjects 5002 }


-- dma.2.5.2.0.6001
ntfAlertConfMgrNoTerritories NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "No territories are configured to host conference rooms; the DMA conference
manager
               cannot process conferences."
    ::= { ntfAlertNotificationObjects 6001 }

-- dma.2.5.2.0.7001
ntfAlertCallServerRegistrationDataIncomplete NOTIFICATION-TYPE
    OBJECTS
    {
       ntfObjAlertID,
       ntfObjAlertTimestamp,
       ntfObjAlertCode,
       ntfObjAlertSeverity,
       ntfObjAlertDescription
    }
    STATUS       current
    DESCRIPTION "History retention settings for registration data limits the period for which
failed
               registrations can be counted to less than 24 hours."
    ::= { ntfAlertNotificationObjects 7001 }
```

```
-- DMA CONFORMANCE

-- dma.2.9
dmaConformance OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Contains conformance objects for the DMA MIB."
    ::= { dmaMonitoring1 9 }


-- .2.9.1
dmaConformanceGroups OBJECT-IDENTITY
    STATUS       current
    DESCRIPTION "Contains conformance groups."
    ::= { dmaConformance 1 }


-- .2.9.1.1
dmaConformanceConfig OBJECT-GROUP
    OBJECTS
    {
--    dmaConfig
--        cfgIdentity
--            cfgProductInfo
                cfgProdInfoManufacturer,
                cfgProdInfoModel,
--            cfgProdInfoHardwareInfo
                    cfgProdInfoHWModel,
                    cfgProdInfoHWSerialNumber,
--            cfgProdInfoSoftwareInfo
                    cfgProdInfoSWVersion,
--            cfgProdInfoSWExtendedVersion
                    cfgProdInfoSWExtVerPlatformVersion,
                    cfgProdInfoSWExtVerApplicationVersion,
--        cfgServer
--            cfgNetwork
                cfgNetworkHostname,
                cfgInterfacesCount,
--            cfgInterfacesTable
--                cfgInterfacesEntry
--                    cfgIfIndex
                    cfgIfName,
                    cfgIfEnabled,
                    cfgIfMACAddress,
                    cfgIfIPv4Address,
                    cfgIfIPv4SubnetMask,
                    cfgIfIPv4Gateway,
                    cfgIfIPv6Address,
                    cfgIfIPv6PrefixLength,
--        cfgCallserver
--            cfgCsSupercluster
--                cfgCsSiteTopology
                    cfgCsTerritoriesCount,
```

```
--                cfgCsTerritoriesTable
--                    cfgCsTerritoriesEntry
--                        cfgCsTerritoryIndex
                             cfgCsTerritoryName,
                             cfgCsTerritoryPrimaryCluster,
                             cfgCsTerritoryBackupCluster,
--            cfgCsIntegrations
--                cfgCsIntDirectoryService
--                    cfgCsIntDirSvcMSActiveDirectory
                             cfgCsIntMSADEnabled,
                             cfgCsIntMSADResponsibleTerritory,
                             cfgCsIntMSADServerAddress,
                             cfgCsIntMSADUserId,
--                cfgCsIntCalendaring
--                    cfgCsIntCalMSExchange
                             cfgCsIntMSExchEnabled,
                             cfgCsIntMSExchResponsibleTerritory,
                             cfgCsIntMSExchServerAddress,
                             cfgCsIntMSExchUserId,
--                cfgCsIntSiteTopology
--                    cfgCsIntSiteTopoPolycomCMA
                             cfgCsIntPlcmCMAEnabled,
                             cfgCsIntPlcmCMAServerAddress,
                             cfgCsIntPlcmCMAUserId,
--                cfgCsIntNetwork
--                    cfgCsIntNetBandwidthManagement
--                        cfgCsIntNetBWMgmtJuniperSRC
                                 cfgCsIntJuniperSRCEnabled,
                                 cfgCsIntJuniperSRCServerAddress,
                                 cfgCsIntJuniperSRCServerPort,
                                 cfgCsIntJuniperSRCUserId,
                                 cfgCsIntJuniperSRCSubscriberURI,
--        cfgCsCluster
--            cfgCsSignaling
--                cfgCsSgnlH323
                         cfgCsSgnlH323Enabled,
                         cfgCsSgnlH323H225Port,
                         cfgCsSgnlH323RASPort,
--                cfgCsSgnlSIP
                         cfgCsSgnlSIPEnabled,
                         cfgCsSgnlSIPTCPPort,
                         cfgCsSgnlSIPUDPPort,
                         cfgCsSgnlSIPTLSPort
--      cfgDevices
   }
   STATUS      current
   DESCRIPTION "Conformance group for dmaConfig."
   ::= { dmaConformanceGroups 1 }


-- .2.9.1.2
```

```
dmaConformanceStatus OBJECT-GROUP
    OBJECTS
    {
--      dmaStatus
--          stServers
                stServerCount,
--          stIdentity
--              stHardwareInfoTable
--                  stHardwareInfoEntry
--                      stHWIndex
                        stHWHostName,
                        stHWSerialNumber,
--              stVersionTable
--                  stVersionEntry
--                      stVerIndex
                        stVerHostName,
                        stVerVersion,
--              stSystemInfoTable
--                  stSystemInfoEntry
--                      stSysInfoIndex
                        stSysInfoHostName,
                        stSysInfoSystemDate,
                        stSysInfoUptime,
                        stSysInfoTimeSource,
--          stNetwork
--              stNetClusterAffiliationTable
--                  stNetClusterAffiliationEntry
--                      stNetClusterAffilIndex
                        stNetClusterAffilHostName,
                        stNetClusterAffilClusterName,
--              stNetPrivateInterfaceTable
--                  stNetPrivateInterfaceEntry
--                      stNetPvtIndex
                        stNetPvtHostName,
                        stNetPvtInterfaceName,
                        stNetPvtLinkStatus,
                        stNetPvtMACAddress,
                        stNetPvtIPv4Address,
                        stNetPvtIPv6Address,
--              stNetManagementInterfaceTable
--                  stNetManagementInterfaceEntry
--                      stNetMgmtIndex
                        stNetMgmtHostName,
                        stNetMgmtInterfaceName,
                        stNetMgmtLinkStatus,
                        stNetMgmtMACAddress,
                        stNetMgmtIPv4Address,
                        stNetMgmtIPv6Address,
--              stNetSignalingInterfaceTable
--                  stNetSignalingInterfaceEntry
```

```
--              stNetSgnlIndex
                stNetSgnlHostName,
                stNetSgnlInterfaceName,
                stNetSgnlLinkStatus,
                stNetSgnlMACAddress,
                stNetSgnlIPv4Address,
                stNetSgnlIPv6Address,
--         stResources
--             stRsrcCPUUsageTable
--                 stRsrcCPUUsageEntry
--                     stRsrcCPUUsageIndex
                       stRsrcCPUUsageHostName,
                       stRsrcCPUUsageCPUUtilizationPct,
--             stRsrcMemoryUsageTable
--                 stRsrcMemoryUsageEntry
--                     stRsrcMemUsageIndex
                       stRsrcMemUsageHostName,
                       stRsrcMemUsageTotalMemory,
                       stRsrcMemUsageBuffersAndCache,
                       stRsrcMemUsageUsed,
                       stRsrcMemUsageFree,
--             stRsrcSwapSpaceTable
--                 stRsrcSwapSpaceEntry
--                     stRsrcSwapIndex
                       stRsrcSwapHostName,
                       stRsrcSwapTotal,
                       stRsrcSwapUsed,
--             stRsrcDiskSpaceTable
--                 stRsrcDiskSpaceEntry
--                     stRsrcDiskIndex
                       stRsrcDiskHostName,
                       stRsrcDiskTotal,
                       stRsrcDiskUsed,
--             stRsrcLogSpaceTable
--                 stRsrcLogSpaceEntry
--                     stRsrcLogIndex
                       stRsrcLogHostName,
                       stRsrcLogTotal,
                       stRsrcLogUsed,
                       stRsrcLogWarningThreshold,
                       stRsrcLogNextPurge,
--     stDevices
--         stMCUs
                stMCUCount,
--             stMCUStatusTable
--                 stMCUStatusEntry
--                     stMCUStIndex
                       stMCUStName,
                       stMCUStServiceStatus,
                       stMCUStHasAlert,
```

```
                             stMCUStRecordingAvailable,
                             stMCUStIVRAvailable,
--              stMCUVideoPortUsageTable
--                  stMCUVideoPortUsageEntry
--                      stMCUVidUsageIndex
                         stMCUVidUsageName,
                         stMCUVidUsageMCUTotal,
                         stMCUVidUsageMCUUsed,
                         stMCUVidUsageDMATotal,
                         stMCUVidUsageDMAUsed,
                         stMCUVidUsageCMAReserved,
--              stMCUVoicePortUsageTable
--                  stMCUVoicePortUsageEntry
--                      stMCUVoxUsageIndex
                         stMCUVoxUsageName,
                         stMCUVoxUsageMCUTotal,
                         stMCUVoxUsageMCUUsed,
                         stMCUVoxUsageDMATotal,
                         stMCUVoxUsageDMAUsed,
--          stMCUsPerCluster
                 stMCUsPerClusterCount,
--              stMCUPCConnectionStatusTable
--                  stMCUPCConnectionStatusEntry
--                      stMCUPCConnStIndex
                         stMCUPCConnStName,
                         stMCUPCConnStClusterName,
                         stMCUPCConnStConnectionStatus,
--              stMCUPCReliabilityStatsTable
--                  stMCUPCReliabilityStatsEntry
--                      stMCUPCRelIndex
                         stMCUPCRelName,
                         stMCUPCRelClusterName,
                         stMCUPCRelDisconnects,
                         stMCUPCRelCallFailureRate,
--      stClusters
             stClustersCount,
--          stClustersTable
--              stClustersEntry
--                  stClIndex
                     stClClusterName,
                     stClClusterStatus,
--          stLicensesTable
--              stLicensesEntry
--                  stLicIndex
                     stLicClusterName,
                     stLicLicenseStatus,
                     stLicLicensedCalls,
                     stLicCallserverActiveCalls,
--      stCallserver
--          stCsSupercluster
```

```
--              stCsSiteTopology
                    stCsConfMgrTerritoriesCount,
--              stCsConfMgrTerritoriesTable
--                  stCsConfMgrTerritoriesEntry
--                      stCsConfMgrTerrIndex
                        stCsConfMgrTerrName,
--          stCsIntegrations
--              stCsIntDirectoryService
--                  stCsIntDirSvcMSActiveDirectory
                        stCsIntMSADEnabled,
                        stCsIntMSADCacheStatus,
                        stCsIntMSADCachingCluster,
                        stCsIntMSADCachingServer,
                        stCsIntMSADConnectionSecure,
                        stCsIntMSADCacheRefreshDate,
                        stCsIntMSADEnterpriseConfRooms,
--              stCsIntCalendaring
--                  stCsIntCalMSExchange
                        stCsIntMSExchEnabled,
                        stCsIntMSExchSubscriptionStatus,
                        stCsIntMSExchIntegratingCluster,
                        stCsIntMSExchIntegratingServer,
                        stCsIntMSExchMailbox,
                        stCsIntMSExchMeetingsToday,
--              stCsIntSiteTopology
--                  stCsIntSiteTopoPolycomCMA
                        stCsIntPlcmCMAEnabled,
                        stCsIntPlcmCMAConnectionStatus,
                        stCsIntPlcmCMALastContactDate,
                        stCsIntPlcmCMATimeSinceLastRefresh,
                        stCsIntPlcmCMATerritories,
                        stCsIntPlcmCMASites,
                        stCsIntPlcmCMASiteLinks,
                        stCsIntPlcmCMAMPLSClouds,
--              stCsIntNetwork
--                  stCsIntNetBandwidthManagement
--                      stCsIntNetBWMgmtJuniperSRC
                            stCsIntJuniperSRCEnabled,
--          stCsDevices
--              stCsConfMgrMCUs
                    stCsConfMgrMCUsCount,
--              stCsConfMgrMCUsTable
--                  stCsConfMgrMCUsEntry
--                      stCsCMMCUIndex
                        stCsCMMCUName
    }
    STATUS      current
    DESCRIPTION "Conformance group for dmaStatus."
    ::= { dmaConformanceGroups 2 }
```

```
--  .2.9.1.3
dmaConformanceUsage OBJECT-GROUP
    OBJECTS
    {
--      dmaUsage
--          useConfHistory
--              useConfHistoryMaximumParticipants
                    useCHMaxPartsLast60MinutesCount,
--              useCHMaxPartsLast60MinutesTable
--                  useCHMaxPartsLast60MinutesEntry
--                      useCHMaxParts60MinIndex
                        useCHMaxParts60MinClusterName,
                        useCHMaxParts60MinTimestamp,
                        useCHMaxParts60MinMaxSimultaneousCalls,
                        useCHMaxParts60MinMaxAdHocCalls,
                        useCHMaxParts60MinMaxPCOCalls,
                    useCHMaxPartsLast24HoursCount,
--              useCHMaxPartsLast24HoursTable
--                  useCHMaxPartsLast24HoursEntry
--                      useCHMaxParts24HrIndex
                        useCHMaxParts24HrClusterName,
                        useCHMaxParts24HrTimestamp,
                        useCHMaxParts24HrMaxSimultaneousCalls,
                        useCHMaxParts24HrMaxAdHocCalls,
                        useCHMaxParts24HrMaxPCOCalls,
                    useCHMaxPartsLast180DaysCount,
--              useCHMaxPartsLast180DaysTable
--                  useCHMaxPartsLast180DaysEntry
--                      useCHMaxParts180DaysIndex
                        useCHMaxParts180DaysClusterName,
                        useCHMaxParts180DaysTimestamp,
                        useCHMaxParts180DaysMaxSimultaneousCalls,
                        useCHMaxParts180DaysMaxAdHocCalls,
                        useCHMaxParts180DaysMaxPCOCalls,
--          useCurrentConferences
--              useCurrentConfsConfManagerUsage
                    useConfMgrUsageCount,
--              useConfMgrUsageTable
--                  useConfMgrUsageEntry
--                      useCMUsageIndex
                        useCMUsageClusterName,
                        useCMUsageActiveConfs,
                        useCMUsageActiveParts,
                        useCMUsageTotalVideoPorts,
                        useCMUsageUsedVideoPorts,
                        useCMUsageTotalVoicePorts,
                        useCMUsageUsedVoicePorts,
                        useCMUsageLocalUsers,
                        useCMUsageCustomConfRooms,
--          useDevices
```

```
--          useDevRegistrations
                useDevRegistrationsCount,
--          useDevRegistrationsTable
--              useDevRegistrationsEntry
--                  useDevRegIndex
                    useDevRegClusterName,
                    useDevRegActiveEndpointReg,
                    useDevRegInactiveEndpointReg,
                    useDevRegFailedEndpointRegLast24Hours
    }
    STATUS      current
    DESCRIPTION "Conformance group for dmaUsage."
    ::= { dmaConformanceGroups 3 }


-- .2.9.1.4
dmaConformanceAlerts OBJECT-GROUP
    OBJECTS
    {
--    dmaAlerts
--        alActiveAlerts
            alActiveAlertsCount,
--          alActiveAlertsTable
--              alActiveAlertsEntry
--                  alActAlertIndex
                    alActAlertID,
                    alActAlertTimestamp,
                    alActAlertCode,
                    alActAlertSeverity,
                    alActAlertDescription
    }
    STATUS      current
    DESCRIPTION "Conformance group for dmaAlerts."
    ::= { dmaConformanceGroups 4 }


-- .2.9.1.5.1         dmaConformanceNtfObjects
-- .2.9.1.5.2         dmaConformanceNtfAlertNotifications
-- .2.9.1.5
dmaConformanceNotifications OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "Contains conformance groups for notifications."
    ::= { dmaConformanceGroups 5 }


-- .2.9.1.5.1
dmaConformanceNtfObjects OBJECT-GROUP
    OBJECTS
    {
--    dmaNotifications
--        ntfObjects
            ntfObjAlertID,
            ntfObjAlertTimestamp,
```

```
            ntfObjAlertCode,
            ntfObjAlertSeverity,
            ntfObjAlertDescription
    }
    STATUS      current
    DESCRIPTION "Conformance group for notification objects."
    ::= { dmaConformanceNotifications 1 }


-- .2.9.1.5.2
dmaConformanceNtfAlertNotifications NOTIFICATION-GROUP
    NOTIFICATIONS
    {
--      dmaNotifications
--          ntfAlertNotifications
--              ntfAlertNotificationObjects
                ntfAlertClusterBusyOut,
                ntfAlertClusterOutOfService,
                ntfAlertClusterOrphan,
                ntfAlertClusterUnreachable,
                ntfAlertClusterPendingReplication,
                ntfAlertTerritoryNotActiveBothClustersNotInService,
                ntfAlertTerritoryNotActiveClusterNotInService,
                ntfAlertTerritoryNoClustersAssigned,
                ntfAlertTerritoryPrimaryClusterNotInService,
                ntfAlertCMAUser,
                ntfAlertCMAUnreachable,
                ntfAlertEntDirIntegrationFailed,
                ntfAlertEntDirNoConfRooms,
                ntfAlertEntDirPrimaryClusterNotInService,
                ntfAlertEntDirNotAvailable,
                ntfAlertEntDirNotAvailableNoBackup,
                ntfAlertEntDirUserAuthConnectionFailed,
                ntfAlertEntDirCachingConnectionFailed,
                ntfAlertExchangePrimaryClusterNotInServiceBackupAvailable,
                ntfAlertExchangeBothClustersNotInService,
                ntfAlertExchangePrimaryClusterNotInService,
                ntfAlertSignalingNotEnabled,
                ntfAlertCertExpired,
                ntfAlertCertExpireNow,
                ntfAlertCertExpireSoon,
                ntfAlertCertSecExpired,
                ntfAlertCertSecExpireSoon,
                ntfAlertLicenseNoKeys,
                ntfAlertLicenseInvalidKeys,
                ntfAlertNetworkSingleNodeDetected,
                ntfAlertNetworkPrivateActive,
                ntfAlertNetworkPrivateError,
                ntfAlertNetworkPublicError,
                ntfAlertNetworkSignalingError,
                ntfAlertResourceDiskSpace,
```

```
                ntfAlertResourceLogsPurge,
                ntfAlertResourceLogsExceedLimit,
                ntfAlertResourceLogsNearLimit,
                ntfAlertResourceCPUOver50Percent,
                ntfAlertResourceCPUOver75Percent,
                ntfAlertAVVirusDetected,
                ntfAlertAVUnsuccessful,
                ntfAlertAVNeverSucceeded,
                ntfAlertDataSyncVersion,
                ntfAlertDataSyncSystemTime,
                ntfAlertDataSyncADIntegration,
                ntfAlertDataSyncADConfRooms,
                ntfAlertDataSyncCustomConfRooms,
                ntfAlertDataSyncLocalUsers,
                ntfAlertMCUBusyOut,
                ntfAlertMCUOutOfService,
                ntfAlertMCUMultipleWarnings,
                ntfAlertITPSystemConfigurationError,
                ntfAlertEndpointSignalingAlert
                ntfAlertConfMgrNoTerritories,
                ntfAlertCallServerRegistrationDataIncomplete
        }
    STATUS       current
    DESCRIPTION "Conformance group for alert notifications."
    ::= { dmaConformanceNotifications 2 }

-- .2.10
dmaCompliance MODULE-COMPLIANCE
    STATUS       current
    DESCRIPTION "Specification of MIB object compliance."
    MODULE       POLYCOM-DMA-MIB
    MANDATORY-GROUPS
    {
        -- .2.9.1.1
        dmaConformanceConfig,
        -- .2.9.1.2
        dmaConformanceStatus,
        -- .2.9.1.3
        dmaConformanceUsage,
        -- .2.9.1.4
        dmaConformanceAlerts,
        -- .2.9.1.5.1
        dmaConformanceNtfObjects,
        -- .2.9.1.5.2
        dmaConformanceNtfAlertNotifications
    }
    ::= { dmaMonitoring1 10 }

END
```

See also:

Index

W

working in system 10

X

X.509 certificates 35
XMPP signaling 73

Z

zone orders, MCU
   See pool orders, MCU
zones, MCU
   See pools, MCU

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com