POLYCOM®

Polycom® CMA™ System Operations Guide

4.1.0 | April 2009 | 3725-77601-001B

Trademark Information

Polycom®, the Polycom logo design, ReadiManager® SE200, SoundStation®, ViewStation®, Vortex®, and VSX® are registered trademarks of Polycom, Inc. Global Management System™, Instructor™ FS, iPower™, PathNavigator™,People+Content™, People on Content™, Polycom Converged Management Application™ (CMA™), Polycom EagleEye™, Polycom HDX 4000™, Polycom HDX 7000™, Polycom HDX 8000™, Polycom HDX 9000™, Polycom HDX 9001™, Polycom HDX 9002™, Polycom HDX 9004™, Polycom MGC™, Polycom RMX 1000™, Polycom RMX 2000™, Polycom RSS™ 2000, Polycom Video Border Proxy™ (VBP™), PowerCam™, SoundStructure™, StereoSurround™, and VS4000™ are trademarks of Polycom, Inc. in the United States and various other countries. Allother trademarks are the property of their respective owners.

Patent Information

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

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

Contents

4 Conference Management Operations

5 Advanced Scheduling Operations

6 Conference and Participant Details

7 Endpoint Management Overview

12 Network Device Management Overview

13 MCU Bridge Management Operations

14 Management Operations for Other Network Devices

15 MCU Bridge Device Details

16 Users and Groups Overview

17 User Management Operations

18 System Reports

19 System Administration Overview

20 Conference Setup Overview

21 Conference Setup Operations

22 Room Overview and Operations

23 Directory Setup Operations

24 Polycom CMA System Setup Overview

25 Server Setting Operations

28 Management & Security Operations

29 Dial Plan Setup

1

Polycom® CMA™ System Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) system and includes these topics:

Features and Capabilities

The Polycom CMA system is an integrated scheduling and device management platform for video conferencing that can include these features:

- The Polycom® Converged Management Application™ (CMA™) Desktop client—an easy-to-use video and audio conferencing application that lets your users see and hear the people they call on their desktop system.
- Automatic device provisioning for dynamically-managed Polycom CMA Desktop clients and Polycom HDX systems
- Scheduled device provisioning for standardly-managed and legacy devices

- Automatic device softupdates for dynamically-managed Polycom CMA Desktop clients and Polycom HDX systems
- Scheduled device softupdates for standardly-managed and legacy devices
- On-demand conferencing using embedded MCUs or external MCUs
- Conference scheduling via the Polycom CMA system Web Scheduler or the optional Polycom Scheduling Plugins for Microsoft® Outlook® or IBM® Lotus® Notes®
- Advanced routing to distribute audio and video calls across multiple media servers (MCUs), creating a single seamless resource pool
- Gatekeeper, alternate, and neighboring gatekeeper functionality
- Access to global user and room directories for on-demand and scheduled calls. Directory services include:
  - Presence and contact list functionality for dynamically-managed devices like Polycom CMA Desktop clients and Polycom HDX systems
  - Global Address Book functionality for standardly-managed devices
  - H.350 and LDAP directory functionality. H.350 defines a directory services architecture for multimedia conferencing for H.323, H.320, SIP and generic protocols.
- Device monitoring and management
- Conference monitoring and management
- An optional high-availability, redundant management server configuration

Polycom CMA System Models

Polycom offers two Polycom CMA system models.

- The single microprocessor Polycom CMA 4000 system supports up to 400 concurrently registered endpoints and 240 concurrent calls. Integration with a corporate directory and an external database is optional. The Polycom CMA 4000 system is not available in redundant configurations.
- The dual microprocessor Polycom CMA 5000 system can support up to 5000 concurrently registered endpoints and 1500 concurrent calls. Integration with a corporate directory (Microsoft Active Directory) and an external database (Microsoft SQL Server) is required. The Polycom CMA 5000 system is available in an optional redundant configuration.

Minimum System Requirements

The *Release Notes* for your model and version of Polycom CMA system describe the minimum system requirements for your system. To find the most current *Release Notes*, go to www.polycom.com/support and navigate to the Polycom CMA system product page (**Documentation > Category: Network > Product: Polycom Converged Management Application**).

Other Requirements

Any scheduled call that requires an external MCU requires a Polycom MGC™ or Polycom RMX™ conferencing platform. Some features and services, such as Conference on Demand service also requires a Polycom MGC or RMX conferencing platform. (Some conferencing features are not supported on the RMX 1000 conferencing platform. For more information, see the *Polycom CMA System Release Notes*.)

Log Into the Polycom CMA System

To log into the Polycom CMA system interface, you need:

- Microsoft Internet Explorer® 6.0+ or 7.0, Mozilla FireFox® 2.x or 3.x, or Apple Safari 3.x
- Adobe® Flash® Player 9.0 or 10.0
- The IP address or host name of the Polycom CMA system server and your username, password, and domain.

When users log into a Polycom CMA system, the system first checks to make sure all essential services are running before allowing users access to the system.

The following situations may occur.

- If all required services are running, users are allowed to access the system.
- If one or more required services are down, but the Apache service has been running for at least seven minutes, users are allowed to access to the system.
- If one or more required services are down, and the Apache service has been running for less than seven minutes, users receive an error message saying, “Login Failed. CMA server is not ready to accept logins. Please wait a few minutes and try again.”

To log into a Polycom CMA system

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

   – If prompted to install the Adobe Flash Player, click **OK**.

   – If you receive an HTTPS **Security Alert**, click **Yes**.

   To eliminate these HTTPS certificate security alerts in the future, see "Automatic Registration Server Addressing" on page 283.

2 When the Polycom CMA system **Log In** screen appears, enter your **Username** and **Password**.

3 If necessary, select a different **Language** or **Domain**.

4 Click **Login**.

   Because the Polycom CMA system is a role-based system, you see only the pages and functions available to your roles.

   If you log in as an administrator, you see the Polycom CMA system **Dashboard**.

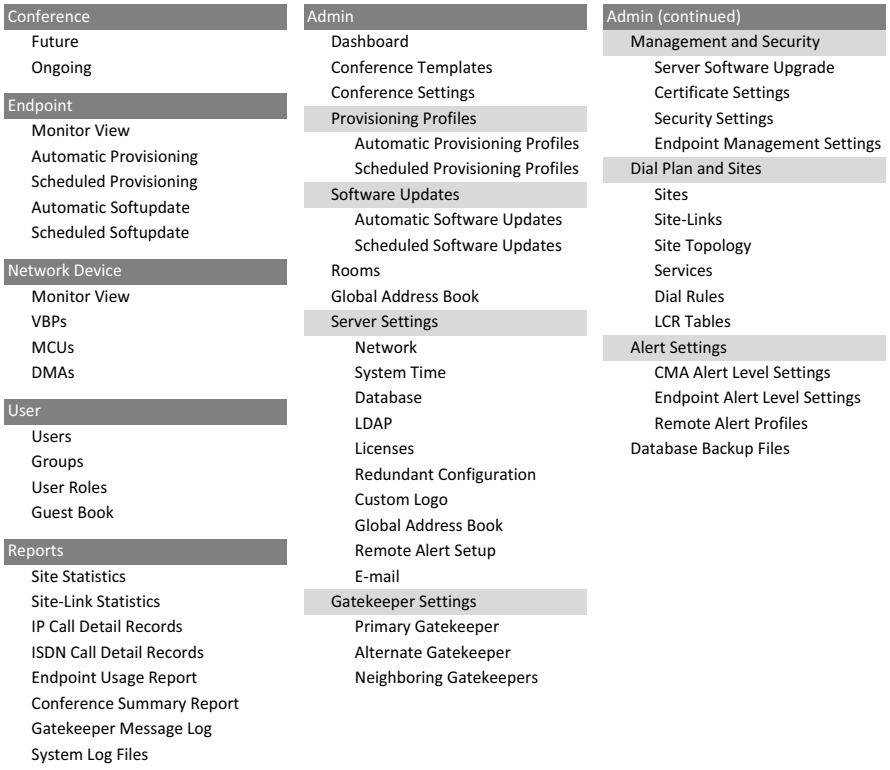
Working in the Polycom CMA System

This section includes some general information you should know when working in the Polycom CMA system. It includes these topics:

- Polycom CMA System Site Map
- Polycom CMA System Views, Roles, and Permissions
- Field Input Requirements
- Filter and Search a List
- Managing Bandwidth

Polycom CMA System Site Map

The following figure shows the Polycom CMA system site map illustrating the organization of the system interface.



Polycom CMA System Views, Roles, and Permissions

When you log into the Polycom CMA system, the view that appears depends on your user roles and the permissions assigned to your user roles.

This section describes the functionality assigned to the default Polycom CMA system user roles. If your Polycom CMA system has been configured with specialized user roles, other pages may appear.

The Polycom CMA system has three default roles: **Administrator**, **Operator**, and **Scheduler**.

- When users who are assigned the default **Scheduler** role log into the Polycom CMA system, they see the **Conference** and **User** menus and the **Future** conference view is displayed. They can schedule, monitor, and manage their own conferences. They can also delete entries from the system Guest Book. They cannot see conferences that they did not create.

- When users who are assigned the default **Operator** role log into the Polycom CMA system, they see the **Conference**, **Endpoint**, **Network Device**, **User**, and **Reports** menus and the **Ongoing** conference view is displayed. They can monitor and manage all ongoing Polycom CMA system conferences; monitor all devices; delete entries from the system Guest Book; and view some system reports.
- When users who are assigned the default **Administrator** role log into the Polycom CMA system, they see the **Endpoint**, **Network Device**, **User**, **Reports,** and **Admin** menus and the system **Dashboard** is displayed. They have access to all Polycom CMA system functionality except that associated with scheduling, monitoring, or managing conferences.

All users see these menu items:

Description
Settings. Click here to display a **Settings** dialog box with the following information: • **User Name** • **Remote Server** • **Software Version** In this dialog box, the user can also change the font size used in their display of the Polycom CMA web client interface.
Downloads. Click here to display the **Downloads** dialog box with the downloadable applications compatible with the Polycom CMA system. Downloadable applications include: • Polycom CMA Desktop client (including the path to the application) • Scheduling Plugin for Microsoft Outlook • Scheduling Plugin for IBM Lotus Notes
Log Out. Click here to log out of the Polycom CMA system. **Note** The Polycom CMA system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time (10 minutes), the system automatically logs you out. To change this inactivity timer, see "Change the Polycom CMA System User Interface Timeout" on page 282.
Help. Links to the Polycom CMA system online help.

For more information about Polycom CMA system roles and permissions, see "Users and Groups Overview" on page 169.

Field Input Requirements

While every effort was made to internationalize the Polycom CMA system, not all system fields accept Unicode entries. If you work in a language other than English, be aware that the Polycom CMA system fields that accept only ASCII characters are shaded a light yellow. For information about specific field requirements, see "System Field Input Requirements" on page 351.

Filter and Search a List

In the Polycom CMA system interface, information is often summarized in lists or grids.

Lists that include many items may have filters or searchable fields, which allow you to view a subset of items or search for a specific entry. The available filtering options depend on the type of information in the list. For example in the conference list:

- If you select **Custom Date** as the filter, a calendar filter field appears
- If you select **Ongoing Plus** as the filter, an attribute option appears. You can select the attribute **Conference Name** and enter all or part of the conference name into the associated text field.

In general, most text filter fields are ASCII only and the Polycom CMA system search function is a case-insensitive, substring search. That means when you enter a search string, the Polycom CMA system looks for that string where ever it occurs (beginning, middle, or end) in the word or number.

However, some Polycom CMA system searches—specifically those searches for users in the enterprise directory—are case-insensitive, exact-match searches. In this case, you must either:

- Enter an exact text match in the field (except for case)
- Use wildcards (*) at the beginning and end of the search string to create a viable substring search

Note

? is not a valid wildcard.

For example, all of the following searches will find Barbara Smithe:

```
Barbara
Smithe
Bar*
Smi*
*ara*
```

But none of the following searches will find Barbara Smithe:

```
Barb
Smith
*Smi
```

Note

Searches on the Polycom CMA system **Users** screen search the **UserID**, **First Name**, and **Last Name** fields.

The following is the complete list of attributes used as criteria by a Polycom CMA system or a Polycom CMA Desktop system when searching Active Directory:

- ObjectCategory
- memberOf
- DisplayName
- GivenName
- Sn
- Cn
- Samaccountname
- groupType
- distinguishedName
- objectGuid

These are requested attributes to be returned by the search:

- Sn
- Givenname
- Mail
- Ou
- Objectguid
- Telephonenumber
- Cn
- Samaccountname
- Memberof
- Displayname
- Objectclass
- Title
- localityName
- department

Managing Bandwidth

The Polycom CMA system manages the bandwidth between sites and the bandwidth for calls that it schedules within the gatekeeper region it services.

Users with administrator permissions can create bandwidth management policies by setting the following limits. The Polycom CMA system applies the lowest value from the settings described here to limit the bit rate of specific calls or conferences.

- **The maximum bit rate for each call at a site.** Set it by editing the site, selecting **Routing/Bandwidth**, and setting the **Call Max Bit Rate**.
- **The total bandwidth between sites.** The link type and bandwidth are parameters of the site links between two sites. Set it by editing the site link. (A call across a multi-site link will use the minimum available bandwidth for all links used for the multi site link.)
- **The maximum speed (bit rate) for calls across a site link.** This value is also a parameter of the site links between two sites and is set by editing the site link. (A call across a multi-site link will use the minimum available bandwidth for all links used for the multi site link.)
- **The specific speed (bit rate) of calls in a conference.** This value is a parameter of the conference, as it is inherited from the conference template. You can achieve granularity of bandwidth management by (a) creating a variety of scheduling roles, (b) creating a variety of conference templates with different conference speeds, (c) associating different scheduling roles with different templates, and (d) associating different users and/or groups with the different scheduling roles.

  For example, you can assign an executive user or group more bandwidth than your typical user. To do this, create a VIP role and assign it scheduling or advanced scheduling permissions. Then create a VIP conference template that has a higher video speed, say 4096 kpbs. Finally, associate the executive user or group with the VIP role.

  There are some things to note in these situations.

  – The Polycom CMA system may reduce bandwidth or fail a call if the requested bandwidth is not available.

  – The gate keeper will reduce bandwidth or fail a call if an endpoint requests a speed higher than what is available. If the available speed is less then 56 kbps, the gate keeper will reject the call.

  – Schedulers with advanced scheduling permissions can choose to change the speed of calls in conference by changing the value for a specific conference. However, the Polycom CMA system only allows a connection speed when it is within the parameters set for the site link.

  – Devices in a conference may not be capable of transmitting at the requested speed. In this case, they will transmit at the value they can achieve that is closest to the value set for the conference.

- **The maximum speed (bit rate) for receiving calls and the preferred speed for placing calls provisioned on the device**. These values are parameters of the device. For devices in dynamic management mode, these values are provisioned as part of the automatic provisioning profile. For devices operating in standard/traditional management mode, these values are provisioned at the device.

  Note in this case that the device can request a speed when placing a call, but again the Polycom CMA system only allows a connection speed when it is within the parameters set for the site topology.

Log Out of the Polycom CMA System

To log out of the Polycom CMA system

>> Click **Log Out** in the top-right corner of the page.

2

Polycom® CMA™ System Configuration

This chapter describes the configuration tasks that may be required, based on your system design, to complete your implementation of a new Polycom® Converged Management Application™ (CMA™) system once **First Time Setup** is complete. It includes these topics:

- Add DNS SRV Record for Polycom CMA Services
- Configure the Connection to the External Database
- Configure the Connection to an External Enterprise Directory
- Configure Redundancy
- Set Up Video Call Routing
- Set Up Automatic Device Provisioning
- Set Up Automatic Softupdate
- Set Up Conference Templates
- Set Up Directory Services
- Distribute Polycom Applications

Add DNS SRV Record for Polycom CMA Services

You must configure your DNS server, if you wish the DNS to resolve queries for the Polycom CMA system by the host name and/or IP address assigned on the **Network** page. The DNS server should also have entries for your Active Directory server (if different from the DNS server) and for the externaldatabase server being used by the Polcyom CMA system.

To implement dynamic management mode, which enables automatic provisioning, automatic softupdate, and presence, you must add the DNS service record (SRV record) for the Polycom CMA system. The lookup key for this service record is `_cmaconfig._tcp` . So the record will resemble this:

```
__cmaconfig._tcp.customerdomain.com 86400 IN SRV 0 443 cma5000.customerdomain.com
```

Configure the Connection to the External Database

If during **First Time Setup** you did not configure your Polycom CMA system to use an external Microsoft SQL Server database, but need to do so now, see "Integrate the Polycom CMA System to an External Database" on page 250.

Note

It is not recommended, but you can create the Polycom CMA system databases manually using Microsoft SQL scripts. Contact Polycom Global Services to request the creation scripts.

Polycom CMA 5000 systems require an external database.

Configure the Connection to an External Enterprise Directory

If during **First Time Setup** you did not configure your Polycom CMA system to use an enterprise directory, but need to do so now, see "Integrate the Polycom CMA System to an Enterprise Directory" on page 251.

Connecting to an enterprise directory allows users to enter their network usernames and password to log into Polycom CMA system. It also allows users to select conference participants from the enterprise directory.

Polycom CMA 5000 systems require an enterprise directory.

Configure Redundancy

You can install the Polycom CMA 5000 system in a fault-tolerant, high-availability, redundant configuration. The Polycom CMA 4000 system is not available in a redundant configuration.

A redundant Polycom CMA system configuration requires the installation of two Polycom CMA system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses and leave them pointed at their internal databases. Once the two system servers are installed, see "Polycom CMA System Redundancy" on page 261.

Set Up Video Call Routing

The video call routing setup includes the gatekeeper, site topology, dial plan, system services, gateway and MCU services, and bandwidth management.

You can perform the following tasks:

- Handle inbound ISDN calls and route them to correct endpoints.
- Enable outbound IP- based calls.
- Connect through a firewall using an SBC device.
- Allow or deny calls to and from unregistered endpoints (rogue calls).
- When you have a third-party MCU that registers with the gatekeeper using standard H.323 protocol, add gateway and MCU services manually.
- Define new sites and site links.
- Add IP-to-ISDN call routing using least-cost routing.
- Define neighboring gatekeepers
- Enable routing of H.323 calls to neighboring gatekeepers
- Define a site for each physical location in which a LAN or an ISDN connection exists. If you use VPN connections, you can consolidate distinct physical locations into a single logical site to simplify management tasks.
- For each site, define the subnets in which the video endpoint systems are deployed.

Note

It is critical that the IP addresses used by the endpoints belong to only one subnet at a site.

- Define least-cost routing tables only when you use the least-cost routing feature.
- Customize default dialing rules.

For more information, see "Dial Plan Setup" on page 285.

Set Up Automatic Device Provisioning

The Polycom CMA system automatic device provisioning feature allows an administrator to configure one or more devices with the standard set of information the registering devices need to operate within the network. This eliminates the need to configure each device individually.

Automatic device provisioning is enabled at the device, but the Polycom CMA system must have automatic provisioning profiles for both the device and the site at which the device resides.

To ensure out-of-box usability, the Polycom CMA system comes with default automatic provisioning profiles. However, to create your desired user experiences, you should:

- Create customized automatic provisioning profiles for the device
- Edit the provisioning profile for the site.

For more information, see "Add an Automatic Provisioning Profile" on page 108.

Set Up Automatic Softupdate

The Polycom CMA system automatic softupdate feature allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each device individually.

The automatic device softupdate feature is enabled at the endpoint. At start up and at designated intervals, endpoints in automatic softupdate mode automatically look for a new softupdate profile and package on the Polycom CMA system.

To implement automatic device softupdates, you must create a softupdate package for each device type you wish to support with updates.

For more information, see "Implement Automatic Softupdates for Endpoints" on page 116.

Set Up Conference Templates

The Polycom CMA system uses conference templates and global conference settings to manage system and conference behavior.

The Polycom CMA system has a **Default Template** and default global conference settings. You may want to create additional templates with different settings or change the global conference settings.

For more information, see "Conference Setup Overview" on page 207.

Set Up Directory Services

Directory services provide information about all users, devices, and resources on your video communication network.

To set up Polycom CMA directory services, complete the following tasks:

1. Register devices. On the device, you must set the gatekeeper and/or Global Directory Server (GDS) to point to the Polycom CMA system IP address or DNS name. We recommend using the IP address to prevent data inconsistencies.

   Most endpoint information is automatically populated in the Polycom CMA system through the gatekeeper or GDS registration. You must review these devices in the Polycom CMA **Directory Setup** page and fill in missing information.

   You can also register endpoints to the directory from the **Admin > Global Address Book** page. Make sure the endpoint is online before you register it.

   To select devices when scheduling conferences, you must first associate them with a user or conference room by editing the specific user or room settings. For more information, see "Endpoint Management Overview" on page 61.

2. Set up users and associate them with endpoints. Unless your Polycom CMA system is integrated with an enterprise directory, you must enter all user information manually including endpoint association. If your system is integrated with an enterprise directory, general user information (**First Name**, **Last Name**, **UserID**, **Password**, **Email Address**) is directly pulled from the directory and cannot be changed. However, you must still associate enterprise users with endpoints. For more information, see "Users and Groups Overview" on page 169.

3. Set up groups, add memebers, and associate them with provisioning profiles. For more information, see "Users and Groups Overview" on page 169.

4. Set up rooms and associate them with devices. Unless your Polycom CMA system is integrated with an enterprise directory that includes conference rooms, you must enter all room information manually including device association. For more information, see "Room Overview and Operations" on page 219.

Distribute Polycom Applications

To deploy the Polycom CMA Desktop client to users within a private enterprise network, you can:

- Copy the link for the **Polycom CMA Desktop** client from the Polycom CMA system **Downloads** page into an email that you can send to users. See "Option 1: Distribute the Polycom CMA Desktop client via an email link" on page 17.
- Provide users access to the Polycom CMA system, from which they can download the client. See "Option 2: Distribute the Polycom CMA Desktop client via the management system" on page 18.
- Distribute the `.exe` installation file as a desktop management or group policy object to a location on client systems and provide directions to users on how to run the executable. See "Option 3: Distribute the Polycom CMA Desktop client via a desktop management or group policy object" on page 19.

IMPORTANT

- On a Windows XP system, the user installing the Polycom CMA Desktop must sign in with administrative privileges. On a Windows Vista system, the user installing the Polycom CMA Desktop must sign into the Administrator account.
- The following procedures assumes you have implemented DNS lookup and Windows authentication for single signon.

Option 1: Distribute the Polycom CMA Desktop client via an email link

To distribute the Polycom CMA Desktop client to users via an email link:

1. Log into the Polycom CMA system and go to **User > Users** to verify that the users have accounts on the system. (Users are typically added through integration with your enterprise directory.)
2. On the task bar, click the **Downloads** link.
3. Copy and paste the **Polycom CMA Desktop (shipped version)** link into an email to be sent to users.
4. Create installation instructions and add them to the email. Edit the following sample instructions (the procedure encased by the dashed lines) for your situation. Include usernames and passwords as required.

To install the Polycom CMA Desktop application from the email link provided

1. Connect a webcam to your computer and install the camera software using the instructions received with the webcam.
2. Click the link provided in this email.
3. Save the software to your local system, and then double-click it. The installation program launches automatically.
4. Follow the instructions to install the software.
5. <***Note to Administrator***—Have users choose **Automatic**, if you have a DNS server record for the Polycom CMA system on your DNS server.>
   a. When prompted for the server location, select **Automatic**.
   b. When prompted for the server location, select **Specify** and enter the following IP address: _____.

   When the installation program is complete, the Polycom CMA Desktop client starts. You will be asked if you would like to sign in using your network credentials.
6. <***Note to Administrator***—Have users choose **Yes**, if your Polycom CMA system is integrated with your enterprise directory.>
   a. Click **Yes** to use your network credentials.
   b. Click **No** to use locally defined credentials.
7. Click **Sign In**. Once the system signs you in, you're ready to connect to anyone else using Polycom CMA Desktop or other video endpoints systems.

Option 2: Distribute the Polycom CMA Desktop client via the management system

To distribute the Polycom CMA Desktop client to users by providing them access to the Polycom CMA system, you must:

1. Log into the Polycom CMA system and go to **User > Users** to verify that the users have accounts on the system. (Users are typically added through integration with your enterprise directory.)
2. Copy and paste the Polycom CMA system IP address or host name into an email to be sent to users.
3. Create installation instructions and add them to the email. Edit the following sample instructions (the procedure encased by the dashed lines) for your situation. Include usernames and passwords as required.

To install the Polycom CMA Desktop application from the Polycom CMA system

1. Connect a webcam to your computer and install the camera software using the instructions you received with the webcam.
2. Open a browser window and in the **Address** field enter the Polycom CMA system server IP address.
   - If prompted to install the Adobe Flash Player, click **OK**.
   - If you receive a **Security Alert**, click **Yes**.
3. When the Polycom CMA system login screen appears, enter your standard network **Username** and **Password**.
4. Click **Login**.
5. From the Polycom CMA system toolbar, click **Downloads**.
6. Click **Polycom CMA Desktop**.
7. Save the software to your local system, and then double-click it. The installation program launches automatically.
8. Follow the instructions to install the software.
9. When prompted for the server location, select **Automatic**.
10. When you are asked if you would like to sign in using your network credentials, click **Yes**.
11. Click **Sign In**.

    Once the system signs you in, you're ready to connect to anyone else using Polycom CMA Desktop or other video endpoints systems.
12. Close the Polycom CMA system **Downloads** screen and click **Log Out**.

Option 3: Distribute the Polycom CMA Desktop client via a desktop management or group policy object

The Polycom CMA Desktop client is a standard `.msi` or `.exe` installation file and as such can be distributed via a desktop management or group policy object should your company have such processes and tools available to it.

To distribute the Polycom CMA Desktop client `.msi` or `.exe` installation file via a desktop management or group policy object, you must:

1. Build a desktop management or group policy object that writes the `.msi` or `.exe` installation file to a directory (for example, `C:\temp`) on the user's local system.
2. Create installation instructions and put them into an email to be sent to users. Edit the following sample instructions (the procedure encased by the dashed lines) for your situation.

To install Polycom CMA Desktop from the .msi file

1. Connect a webcam to your computer and install the camera software using the instructions received with the webcam.
2. Choose **Start > Run**.
3. Enter this command:

   ```
   msiexec /qn /i "C:\temp\CMA Desktop.msi"
   ```

4. Follow the instructions to install the software.
5. When prompted for the server location, select **Automatic**.

   When the installation program is complete, the Polycom CMA Desktop client starts. The **Sign In** screen displays your ***<DOMAIN>**<username>*** in the **Sign in as** field.
6. Click **Sign In**.

   Once the system signs you in, you're ready to connect to anyone else using Polycom CMA Desktop or other types of video conferencing systems.

Option 4: Distribute the Polycom CMA Desktop client via a .zip file

To distribute the Polycom CMA Desktop client `.msi` or `.exe` installation file via a `.zip` file, you must:

1. Download the `.msi` or `.exe` installation file to a local system.
2. Create a `.zip` file using your favorite compression tool.
3. Create installation instructions and put them into an email with the `.zip` file to be sent to users. In the email, you must also include the IP address of the Polycom Video Border Proxy system.

   Edit the following sample instructions (the procedure encased by the dashed lines) for your situation.

To install Polycom CMA Desktop from the .zip file

1. Connect a webcam to your computer and install the camera software using the instructions received with the webcam.
2. Save the `.zip` file to your local system.
3. Extract the `.msi` or `.exe` installation file from the `.zip` file.
4. Run the installation file.
5. Follow the instructions to install the software.
6. When prompted for the server location, select **Specify** and enter the following IP address: _____

   When the installation program is complete, the Polycom CMA Desktop client starts. The **Sign In** screen displays your ***<DOMAIN>**<username>*** in the **Sign in as** field.
7. Click **Sign In**.

   Once the system signs you in, you're ready to connect to anyone else using Polycom CMA Desktop or other types of video conferencing systems.

3

Conference Scheduling Overview

This chapter describes the scheduling and conference views, navigation, and commands of the Polycom CMA system. It includes these topics:

Conference Menu and Views

The Polycom CMA system **Conference** menu provides these views of the **Conference** list:

- **Future**—Displays the list of future conferences in the main window. Use this view to view and edit future conferences.
- **Ongoing**—Displays the list of active conferences in the main window. Use this view to work with ongoing conferences.

The **Conference** views have these sections.

Section	Description
Views	The views you can access from the page
Actions	The set of available commands. The constant commands in the **Conference** views are: • **Refresh** —Use this link to update the display with current information • **Add** —Use this link to create a new video and/or audio conference.

Section	Description
Conference List	The context-sensitive **Conference** list for the selected view
Conference Details	Displays information about the selected conference. For more information, see "Conference Details" on page 53.
Conference Features	Displays the status of system features for the selected conference. For more information, see "Conference Features" on page 55.
Bridge (MCU) Features	Displays the status of MCU features for the selected conference. For more information, see "Bridge (MCU) Features" on page 56.
Participants	Displays the list of participants for the selected conference. For more information, see "Participants" on page 57.
Participant Details	Displays information about the participant selected in the **Participants** list. For more information, see "Participant Details" on page 57.

Conference Views—Future and Ongoing

The **Conference** list in both the **Future** and **Ongoing** view has these fields.

Field	Description
Filter	Use the filter choices to display other views of the conference list, which include: • **Future Only** - Displays scheduled conferences that have not yet started • **Today Only** - Displays scheduled conferences (completed, active, or future) for the current day and active ad hoc conferences • **Custom Date** - Displays scheduled conferences (completed, active, or future) for a selected day. Select the day from the calendar.
Filter (*continued*)	• **Ongoing Plus** - Displays active and future conferences for the day. You can further filter this request by **Owner**, **Conference Name**, and **Endpoint Name**. • **Today Plus** - Displays scheduled conferences (completed, active, or future) for the current day, current ad hoc conferences, and all future conferences. You can further filter this request by **Owner**, **Conference Name**, and **Endpoint Name**. • **Yesterday Plus** - Displays completed scheduled conferences for yesterday and earlier. You can further filter this request by **Owner** and **Conference Name**. For information on filters, see "Filter and Search a List".

Field	Description
Status	The state of the conference. For more information, see "Conference States" on page 24.
Type	The type of scheduled conference. Possible values include: • **Video Conference** —All conference participants have video endpoints • **Audio Only Conference** —All conference participants have audio endpoints. Audio only conferences require an MCU. • **Recurring Conference** —The conference is one in a recurring series
Name	The user-assigned name of the conference. The system appends the day and date to assigned name.
Start Time	The user-assigned start time for the conference. The system appends the time difference between the local time and the standard time.
Bridge	If applicable, the user-assigned bridge for the conference. Possible values are: • **N/A**—A bridge is not required for the conference • **Single Bridge**—The user assigned the conference to a single bridge. The bridge name is displayed. • **Multi bridge** —The user assigned the conference to multiple bridges and created bridge links.
Owner	The conference creator

Conference States

Conferences may be in the following states.

State	Description
Future Conference	Scheduled conference that has not yet started. This conference status is possible in all views except the Yesterday Plus view.
Completed Conference	A scheduled or ad hoc conference that occurred in the past. This conference status is possible in all views except the Future and Ongoing Plus view.
Active Conference	A conference that is still active/ongoing. This conference status is possible in all views except the Future and Yesterday Plus view.
Active Alerts Conference	The bridge on which the active/ongoing conference is being hosted has sent an alert. Examples of events that will trigger a bridge alert are: • A participant is connected in secondary mode (audio only) • A conference is not yet full (i.e., not all scheduled participants have joined the conference)
Declined Conference	Applies only to conferences scheduled through the Polycom Scheduling Plugin for Microsoft Outlook. This state indicates that most participants did not accept the conference invitation.
Conference End Warning	The conference is ending, i.e., it is in its last five minutes unless someone extends it.

Context-Sensitive Conference Commands

Besides the constant **Refresh** and **Add** commands, the **Actions** section may include these context-sensitive commands depending on the type of conference selected.

Command	Description
Available for future conferences only	
Edit	Use this command to edit the selected conference. For more information, see "Edit a Conference" on page 35.
Available for future and past conferences	
Delete	Use this command to delete the selected conference
Available for future, past, and active conferences	
Copy	Use this command to copy the selected conference.

Command	Description
Available for active conferences only	
Manage	Use this command to display the **Manage Conference** page for the conference selected in the **Conference List**. Use this command to manage participants and devices in the selected active conference. For more information, see "Manage an Active Conference" on page 39.
Terminate	Ends the selected conference

General Scheduling Information

You may find the following general topics useful when you are scheduling conferences.

- Bridge Selection and Cascading
- Bridge Scheduling and Reassignment

In the Polycom CMA system interface, information is often summarized in lists or grids.

Lists that include many items may have filters or searchable fields, which allow you to view a subset of items or search for a specific entry. The available filtering options depend on the type of information in the list. For example in the conference list:

- If you select **Custom Date** as the filter, a calendar filter field appears
- If you select **Ongoing Plus** as the filter, an attribute option appears. You can select the attribute **Conference Name** and enter all or part of the conference name into the associated text field.

In general, most text filter fields are ASCII only and the Polycom CMA system search function is a case-insensitive, substring search. That means when you enter a search string, the Polycom CMA system looks for that string where ever it occurs (beginning, middle, or end) in the word or number.

However, some Polycom CMA system searches—specifically those searches for users in the enterprise directory—are case-insensitive, exact-match searches. In this case, you must either:

- Enter an exact text match in the field (except for case)
- Use wildcards (*) at the beginning and end of the search string to create a viable substring search

Note

? is not a valid wildcard.

For example, all of the following searches will find Barbara Smithe:

```
Barbara
Smithe
Bar*
Smi*
*ara*
```

But none of the following searches will find Barbara Smithe:

```
Barb
Smith
*Smi
```

Note

Searches on the Polycom CMA system **Users** screen search the **UserID**, **First Name**, and **Last Name** fields.

The following is the complete list of attributes used as criteria by a Polycom CMA system or a Polycom CMA Desktop system when searching Active Directory:

- ObjectCategory
- memberOf
- DisplayName
- GivenName
- Sn
- Cn
- Samaccountname
- groupType
- distinguishedName
- objectGuid

These are requested attributes to be returned by the search:

- Sn
- Givenname
- Mail
- Ou
- Objectguid
- Telephonenumber
- Cn
- Samaccountname
- Memberof
- Displayname
- Objectclass
- Title
- localityName
- department

Bridge Selection and Cascading

When a conference is scheduled with one of the Polycom CMA system scheduling applications (Web Scheduler, Outlook Scheduler, or Lotus Notes Scheduler), by default the system automatically assigns the conference to a bridge. However, the system allows users with advanced scheduler permissions to select a bridge for their conferences. It also allows them to create multibridge, cascaded conferences.

Bridge Selection

When scheduling a conference, users with advanced scheduler permissions can select a bridge to host their conference by selecting the **Single Bridge** option. When they select this option, the system presents a list of bridges that have the capabilities and resources required to host their conference.

Because this bridge list depends on the template selection and conference settings, users should make their template selection and conference settings before selecting a bridge. Otherwise, they may select a bridge that cannot meet their conferencing requirements. In this case, the system will override their bridge selection and select a bridge that can meet the conferencing requirements. However, the bridge the system selects may not be the bridge the user prefers.

Bridge Selection and Cascading Conferences

When scheduling a conference, users with advanced scheduler permissions can select the **Multi Bridge** option to create cascading conferences.

In some respects, a cascaded conference looks like a single conference, but it is actually two or more conferences on different bridges that are linked together. The link is created by a dial-out from one conference to a second conference via a special cascaded entry queue.

Some reasons you may wish to create cascading conferences include:

- To invite more conference participants than any single bridge can host
- To connect different bridges at different sites into a single conference
- To use the different capabilities of different bridges (for example, different communication protocols, such as, serial connections, ISDN, etc.)

When you create a multibridge, cascaded conference, you must manually select bridges and create the cascaded links between bridges by identifying the originating bridge, the terminating bridge, and the network type (IP or ISDN). The system displays an interconnection diagram that illustrates the cascaded links. Once scheduled, each cascaded link appears as a participant in the conference.

By default, the system automatically assign participants to the “best bridge” for them based on available capacity, location, and least cost routing rules. However, you may also choose to manually assign participants to bridges.

Bridge Scheduling and Reassignment

When a conference is scheduled with one of the Polycom CMA system scheduling applications (Web scheduler, Outlook scheduler, or Lotus Notes scheduler), by default the system automatically assigns the conference to a bridge unless a user with advanced scheduler permissions intercedes. If that bridge is down at the time the system starts the conference, the Polycom CMA system attempts to dynamically reassign the conference to another bridge with sufficient capabilities and resources.

- If the system can successfully reassign the conference to another bridge, the conference starts on the newly selected bridge, and the system sends an updated conference email to all scheduled participants. This updated email includes a new dial-in number that dial-in participants must use to join the conference.
- If the system cannot successfully reassign the conference to another bridge, the conference fails to start. The system sends an email to notify the conference organizer of the failure.

Some notes about bridge reassignment:

- The bridge reassignment process only occurs when the system detects that a bridge is down. It does not occur if the system determines that a bridge does not have sufficient resources required to host the conference.
- If the Polycom CMA system cannot find another bridge with the features and capacity needed to support a conference, the conference fails to start. The system does not attempt to modify the conference settings in any way. Instead, the system sends an email to notify the conference organizer of the failure.
- The system will chain bridge reassignments. This means that if the next bridge to which the system assigns a conference is down at the time the system tries to start the conference, the system will try to reassign the conference again.
- If the bridge to which the system reassigns a conference has ad hoc conferences on it, the Polycom CMA system is unaware of those conferences. The reassigned conference may fail to start if ad hoc conferences are consuming resources the Polycom CMA system expected to schedule. This is known behavior and is avoided by applying the best practice of not using bridges for both scheduled and ad hoc conferences.

4

Conference Management Operations

This chapter describes the Polycom® Converged Management Application™ (CMA™) system conference management operations. It includes these topics:

Add a Conference

To add a new conference

1. Go to **Conference** > **Future** and click **Add**  .
2. In the conference scheduling page, enter a **Conference Name** and set a conference **Start Date**, **Start Time**, and either an **End Time** or **Duration**.
3. To make the conference recurring:
   a. Click **Recurrence** and in the **Appointment Recurrence** dialog box, set:
      - » Recurrence frequency (**Daily**, **Weekly**, or **Monthly**)
      - » Recurrence range (**Start** date and **End After** occurrences or **End by** date)

      The maximum number of recurrences is 52.

b Click **OK**.

4 For a **Video** conference, you can change the template by clicking **Default Template** and selecting a different template.

Note

Conference templates provide default conference settings. When you select a different template, you are changing the default conference settings for your conference.

5 For an **Audio Only** conference:

a Change the **Conference Type** to **Audio Only**.

b You can change the template by clicking **Default Audio Template** and selecting a different template.

6 To add conference participants from the local directory, enterprise directory, or Global Address Book:

a Enter all or part of a participant's **Last Name** or **First Name** into one of the name fields and click **Add Participants**.

The **Add Participants** dialog box appears with the list of participant names that meet your search criteria.

Notes

- Depending on the search domain, the search function may return different results. See Filter and Search a List.
- The search results only include users associated with devices.

b Select the participant's name from the list.

The participant's name appears in the underlying **Selected Participants and Rooms** list.

c Repeat steps a and b to add all domain participants and then click **Close**.

7 To add a guest from the Guest Book:

a Click **Add From Guest Book**.

b In the **Add From Guest Book** dialog box, select the guest's name from the list and click **Close**.

The guest's name appears in the underlying **Selected Participants and Rooms** list.

c Repeat steps b to add all participants from the Guest Book and then click **Close**.

8 To add new guest participants (participants not available from the local directory, enterprise directory, Global Address Book, or Guest Book):

a Click **Add Guest**.

b In the **Add Guest** dialog box, enter the participant's **Name, Email** address, and **Location**. Note that the **Email** address field is ASCII only. For more information, see "Field Input Requirements" on page 6.

c Specify how the participant will join the conference.

Setting	Description
In Person	The participant will attend the conference by going to a room that is included in the conference or joining another participant who is attending the conference.
Audio Only (Dial-In Bridge)	The participant will attend the conference by calling into the conference using the telephone number provided by the system.
Use Video	The participant will attend the conference using a video endpoint system.

d For a guest with an audio endpoint, set **Dial Type** to **IP** or **ISDN** as required.

e For a guest with a video endpoint system:

» Set the **Bit Rate, Dial Options**, and **Dial Type** as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.

» If you select **Dial Out** and a **Dial Type** of **IP**, enter the guest's phone **Number**.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system must use a specific dialing prefix to call the guest, select **Use Modified Dial Number** and enter the guest's complete phone number including prefix, country code, area or city code, and phone number.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system does not need to use a specific dialing prefix to call the guest, select the appropriate **Country** and enter the guest's **Area/City Code** and phone **Number**.

f Select **Save to Guest Book** to have this guest participant added to the system Guest Book.

g Click **OK**.

The guest's name appears in the **Selected Participants and Rooms** list.

9 Adjust the conference date and time as needed to match participant and device availability.

a Review their availability and adjust the conference date and time as needed.

Notes

- For participants who are associated with endpoints, the Polycom CMA system schedules their availability according to the endpoint's availability.
- For participants with multiple endpoints, you must check the availability for each endpoint. Click **Call Info** to change the participant's endpoint.

b To edit a participant's dial settings, select the participant from the **Selected Participants and Rooms** list and click **Edit**. For more information on editing participants settings, see step 5 on page 37.

10 To add conference rooms to the **Selected Participants and Rooms** list:

a Click **Select Site**.

b Select the site of interest from the site list

The conference room list for the selected site appears.

c Select the conference room of interest from the list.

The conference room name appears in the underlying **Selected Participants and Rooms** list.

d Repeat steps b and c to add all required conference rooms and then click **OK**.

11 Once you've added your participants, you can assign them leadership roles:

a To assign a participant the lecturer role, in the **Lecturer** field select the participant's name from the list.

b To assign a participant the video chairperson role, in the **Video Chairperson** field select the participant's name from the list.

Notes

- If the **Lecturer** or **Video Chairperson** options are not available, then the selected template does not support these features.
- To be assigned **Lecturer**, a participant must have a managable video endpoint.

12 If you have advanced scheduler permissions, now is the time to edit conference settings and make bridge selections. For more information, see "Advanced Scheduling Operations" on page 45.

13 When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification email appears with a message indicating **Conference Successfully Scheduled**.

14 To exit without sending an email to your participants, click **Skip Email**.

15 To send an email notification to your participants:

a Copy additional people on the notification and/or add notes about the conference.

Note that the **To**, **CC**, and **BCC** fields are ASCII only. For more information, see "Field Input Requirements" on page 6.

b Click **Send**.

The system sends the conference notification email. The **Future** view appears. Your conference appears in the conference list.

Edit a Conference

You can edit future conferences. You cannot edit active or past conferences.

To edit a future conference

1 Go to **Conference > Future**.

2 Select the conference of interest and click **Edit**  .

3 If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click **Edit**.

The conference scheduling page appears.

4 If you used a template other than the default when you created the conference, reselect the original template.

Note

Once a conference is scheduled, editing the conference and selecting a different template does not change the conference settings. The Polycom CMA system does not store the template as part of the conference information, only the settings selected when the conference was created. To use a different template, you must delete and recreate the conference.

5 Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see "Add a Conference" on page 31.

6 When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification email appears with a message indicating **Conference Successfully Scheduled**.

7 To exit without sending an updated email to your participants, click **Skip Email**.

8 To send an updated email to your participants:

a Copy additional people on the notification and/or add notes about the conference.

Note that the **To**, **CC**, and **BCC** fields are ASCII only. For more information, see "Field Input Requirements" on page 6.

b Click **Send**.

The system sends the updated conference notification email. The **Future** view appears. Your conference appears in the conference list.

Copy a Conference

You can copy future, ongoing, or past conferences.

To copy a conference

1 Go to **Conference > Future**.

2 Select the conference of interest and click **Copy**  .

3 If you used a template other than the default when you created the conference, reselect the template.

Note

Once a conference is scheduled, editing the conference and selecting a different template does not change the conference settings. The Polycom CMA system does not store the template as part of the conference information, only the settings selected when the conference was created. To use a different template, you must delete and recreate the conference.

4 Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see "Add a Conference" on page 31.

5 When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the conference notification email appears with a message indicating **Conference Successfully Scheduled**.

6 To exit without sending an updated email to your participants, click **Skip Email**.

Edit a Participant's Settings

You can edit a participant's settings for future scheduled conferences. You cannot edit a participant's settings for an active or past conference.

To edit a participant's settings

1 Go to **Conference > Future**.

2 Select the conference of interest and click **Edit**  .

3 If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click **Edit**.

4 In the conference scheduling page, select the participant of interest from the **Selected Participants and Rooms** list and click **Edit**.

5 In the **Edit Participant Settings** dialog box, edit the participant settings as required.

a Select the participant's endpoint, if the participant has more than one available.

b Specify how the participant will join the conference.

Setting	Description
In Person	The participant will attend the conference by physically joining another participant who is attending the conference.
Audio Only (Dial-In Bridge)	The participant will attend the conference by calling into the conference using the telephone number provided by the system.
Use Video	The participant will attend the conference using a video endpoint system.

c For a participant with an audio endpoint, set **Dial Type** to **IP** or **ISDN** as required.

d For a participant with a video endpoint:

» Set the **Bit Rate, Dial Options**, and **Dial Type** as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.

» If you select **Dial Out** and a **Dial Type** of **IP**, enter the guest's phone **Number**.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system must use a specific dialing prefix to call the guest, select **Use Modified Dial Number** and enter the guest's complete phone number including prefix, country code, area or city code, and phone number.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system does not need to use a specific dialing prefix to call the guest, select the appropriate **Country** and enter the guest's **Area/City Code** and phone **Number**.

6 Click **OK**.

Edit a Room's Settings

You can edit a room's call settings for future scheduled conferences. The changes apply only to the selected conference.

To edit a room's settings

1 Go to **Conference > Future**.

2 To delete a past conference, select the appropriate filter (such as **Yesterday Plus**).

3 Select the conference of interest and click **Edit**  .

4 If you select a recurring conference, a dialog box appears asking if you want to edit all conferences in the series or just the selected one. Make the appropriate choice and click **Edit**.

5 In the conference scheduling page, select the room of interest from the **Selected Participants and Rooms** list and click **Edit**.

6 In the **Edit Room Settings** dialog box, edit the room settings as required. You can edit:

a Select the room's endpoint, if the room has more than one available.

b For a room with an audio endpoint, set **Dial Type** to **IP** or **ISDN** as required.

c For a room with a video endpoint:

» Set the **Bit Rate, Dial Options**, and **Dial Type** as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.

» If you select **Dial Out** and a **Dial Type** of **IP**, enter the room's phone **Number**.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system must use a specific dialing prefix to call the room, select **Use Modified Dial Number** and enter the room's complete phone number including prefix, country code, area or city code, and phone number.

» If you select **Dial Out** and a **Dial Type** of **ISDN** and the system does not need to use a specific dialing prefix to call the room, select the appropriate **Country** and enter the room's **Area/City Code** and phone **Number**.

7 Click **OK**.

Manage an Active Conference

The **Manage Conference** page provides a detailed view of a single active conference.

To manage an active conference

1 Go to **Conference > Ongoing**.

2 Select the conference of interest and click **Manage** .

The conference page appears displaying the **Participants** list.

3 Use these conference commands as needed:

Command	Use this command...
Terminate	To end an active conference
Extend Duration	To extend the duration of an active conference.
Change Layout	To change the default video layout for the conference display.

Add Participants to an Active Conference

To add additional conference participants to an active conference

1 From your local directory, enterprise directory, or Global Address Book:

a Click **Add Participant** .

b Enter all or part of a participant's **Last Name** or **First Name** into one of the name fields and click **Search**.

A list appears of participant's names that meet your search criteria.

Notes

- Depending on the search domain, the search function may return different results. See "Filter and Search a List" on page 7.
- The search results only include users associated with devices.

c Select the participant's name from the list.

The participant's name appears in the underlying **New Conference Participants** list.

d Repeat steps a and b to add all domain participants and then click **Close**.

e If necessary, edit the new participants' settings. See "Edit a Participant's Settings" on page 37.

Note

Dial Out is the only **Dial Option** the system allows for active conferences.

2 To add new guest participants (participants not available from the local directory, enterprise directory, or Global Address Book):

a Click **Add Participant**  and then click **Add Guest**.

b In the **Add Guest** dialog box, enter the participant's **Name, Email** address, and **Location**. Note that the **Email** address field is ASCII only. For more information, see "Field Input Requirements" on page 6.

c Specify how the participant will join the conference.

Setting	Description
In person	The participant will attend the conference by physically joining another participant who is attending the conference.
Use Video	The participant will attend the conference using a video endpoint system.

d For a guest with a video endpoint:

» Set the **Bit Rate** and **Dial Type** as required. You can change the connection speed for an endpoint up to the maximum speed specified by the conference template.

» If you select a **Dial Type** of **IP**, enter the guest's phone **Number**.

» If you select a **Dial Type** of **ISDN** and the system must use a specific dialing prefix to call the guest, select **Use Modified Dial Number** and enter the guest's complete phone number including prefix, country code, area or city code, and phone number.

» If you select a **Dial Type** of **ISDN** and the system does not need to use a specific dialing prefix to call the guest, select the appropriate **Country** and enter the guest's **Area/City Code** and phone **Number**.

e Select **Save to Guest Book** to have this guest participant added to the system Guest Book.

f Click **OK**.

The participant's name appears in the underlying **New Conference Participants** list.

g If necessary, edit the new participants' settings. See "Edit a Participant's Settings" on page 37.

3 To dial out to new participants, select the participants of interest from the **New Conference Participants** list and click **Connect New Participants**.

Note
Dial Out is the only Dial Option the system allows for active conferences.

Manage a Participant's Device During a Conference

The **Manage** page also allows you to manage conference participant's endpoints. Essentially, you become the conference moderator.

Notes
- These context-sensitive commands only appear when the participant's endpoint supports the action.
- These commands work for rooms on the participant list as well.

To manage a participant's device

1 Go to **Conference > Ongoing**.

2 Select the conference of interest and click **Manage**  .

The **Participants** list appears. It displays these participant settings:

Section	Description
Status	The state of the participant's connection. Possible states include: • Connected • Idle • Help request • Updating • New dial-in participant • New dial-out participant
Type	The type of conference. Possible values include: • Audio Only • Video • VIP
Name	The participant's name
Device	The name assigned to the participant's endpoint when it was added to the system
Mute	The state of the participant's audio connection. Possible values include: • Muted by other • Self muted • Not muted
Access	The endpoint's network interface type. Possible values include: • H323 • ISDN
Address	The IP address or ISDN number of the participant's endpoint (if a dial-out)
Bit Rate	The audio or video data transfer rate (in kbps) of the participant's endpoint
Dial Mode	How the participant joined the call. Possible values include: • Dial-In • Dial-Out

3 Use these conference commands as needed:

Command	Use this command...
Mute or Unmute Audio	To mute or unmute the selected participant's audio feed to the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.
Block or Unblock Video	To block or unblock the selected participant's video feed to the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.
Connect or Disconnect	To disconnect or reconnect the selected participants feed to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.
Remove	To remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.
Send Message	(Users with administrator or operator permissions only) To send a message to the selected participant's registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.
Acknowledge Help	(Users with administrator or operator permissions only) To acknowledge a request for help and send a message to the requesting endpoint.

Terminate an Active Conference

To terminate an active conference

1 Go to **Conference > Ongoing**.

2 Select the conference of interest and click **Terminate** .

3 Click **Terminate** to confirm the termination.

Delete a Conference

You can delete future or past conferences. You cannot delete active conferences.

To delete a conference

1. Go to **Conference > Future**.
2. To delete a past conference, select the appropriate filter (such as **Yesterday Plus**).
3. Select the conference of interest and click **Delete**  .
4. If you select a recurring conference, a dialog box appears asking you if you want to delete just the conference you selected or all conferences in the series. Make the appropriate choice. Active conferences in the series cannot be deleted.
5. Click **Delete** to confirm the deletion.

   The conference is deleted. For future conferences, the system emails the change to the conference owner and participants and releases the participant and room resources.

5

Advanced Scheduling Operations

This chapter describes how users with advanced scheduler permissions have more options when scheduling conferences using the Polycom® Converged Management Application™ (CMA™) system.

When scheduling conferences, users with advanced scheduler permissions can:

- Edit Conference Settings
- Select a Bridge for a Conference
- Create a Cascaded Conference Across Multiple Bridges

Edit Conference Settings

If you have advanced scheduler permissions, you can overwrite certain conference template settings as described here. However, be careful when doing so. If you have an environment with mixed MCU types (e.g., with both Polycom MGC and RMX systems), and the conference you schedule is hosted on a Polycom RMX 2000 system, some of the settings you specify here may be overridden by the RMX profile.

Notes

- A profile is a collection of advanced conference settings that reside on the MCU (Polycom MGC or RMX system). Only an RMX profile can override conference template settings.
- Two conferences scheduled with the same template may have different settings and behavior if they land on different types of MCUs. You can minimize or eliminate such differences by ensuring that all MCUs are similarly configured and that all Polycom CMA system templates are synchronized with RMX profiles.

You can edit conference settings only for scheduled conferences. You cannot edit conference settings for active conferences.

To edit the conference settings

1 On the conference scheduling page, as you are adding or editing a conference, click **Edit Conference Settings**.

2 As needed, configure these settings on the **Conference Settings** dialog box. The settings that you can edit may depend on the template selected.

Setting	Description
Conference Password	The system assigns a four-digit **Conference Password** and provides this password to participants within the content of the conference notification email. You can change this password to another four-digit number.
Enable Chairperson	You can select a video chairperson to control the conference from his or her video endpoint system. The video chairperson must have a video endpoint system and Chairperson conferences require an MCU. **Notes** • If the conference template has the **Conference Requires Chairperson** parameter enabled, then **Enable Chairperson** is automatically selected and cannot be changed. • If a conference is scheduled on a Polycom RMX 2000 system and the RMX profile has **Conference Requires Chairperson** selected but the template does not, and the conference is scheduled without a chairperson, then all users will remain in the waiting **room** and will not be able to join the conference. • Polycom RMX 1000 systems do not support the **Chairperson** feature.
Chairperson Password	If **Enable Chairperson** is selected, the chairperson must enter this four-digit password at their endpoint to assume control. The system sends a separate email with this password to the video chairperson. It is not included in the conference notification email.

Setting	Description
Dial Options	You have three options: • To create a conference for which the same dial-in information and a PIN code are assigned to all conference participants, use the **Dial-In** setting. This setting allows participants to dial in from an audio or video endpoint and connect to the same conference on the MCU. • To dial out to all participants in the conference, use the **Dial-Out** setting. • To allow participants both options, select **Dial-In+Dial-Out**. **Note** When you change a conference from **Dial-In** to **Dial In+Dial Out**, the selected resources remain set to **Dial-In**. You must change them manually.
Always Use MCU	This setting forces the conference to an MCU and prevents video endpoints from connecting to each other directly. This setting is automatically selected and cannot be changed when **Audio Only** is the conference type or when **Enable Chairperson** is selected.
Video Mode	Determines the initial layout on a video endpoint's monitor for a multipoint conference that requires an MCU. The options are: • **Switching.** Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. • **Continuous Presence.** Displays several panels on the monitor, each showing a different participant, and allows you to see all meeting participants at once. You can select a specific layout, with a certain number of windows open. • **Automatic Layout** is a continuous presence layout, in which the number of participants determines the number of panels.
Bit Rate	Specifies the maximum connection speed for endpoints in the conference. Individual endpoints that specify a lower connection speed connect at that lower speed. Endpoints that specify a higher connection speed connect at the speed identified in the conference template. If you select a higher speed than an endpoint can support, the speed for that endpoint is reduced; however, the conference uses the default connection speed for endpoints that can match it. If you place the calls through an endpoint with an embedded MCU, the behavior depends on the capabilities of that endpoint.

Setting	Description
Bit Rate (*continued*)	When the dial speed is higher than the number of channels defined in the H.320 service for the endpoint, you receive a warning. To continue, lower the dial speed to less than or equal to the ISDN capability of the endpoint. Higher speed is important for high-quality video in a meeting. Because higher speeds use greater bandwidth, scheduling a high-bandwidth meeting may limit the number of conferences that you can reserve at one time. **Note** The bit rate can be set at the network level, the device level, and the conference level. If there is a discrepancy between these bit rate settings, the system implements the lowest bit rate setting. The only exception, is that the bit rate in the RMX profile takes precedence over the bit rate in the conference settings.
People + Content	Controls the ability for one endpoint to send two types of data—a data stream and a video stream—over the same bandwidth to display people and content. The receiving endpoint handles the two video streams differently and may display on separate screens or through the video switching mode. Endpoints that do not support the selected method connect with either video through IP or audio only through ISDN. Select from these available settings: • **None.** Select this option when dual data streams are not required. • **People +Content.** This enables the industry standard H.239 dual streams for endpoints that support H.239 or the Polycom proprietary People+Content dual streams for older Polycom endpoints without H.239 capabilities. • **People and Content VO.** This Polycom proprietary technology works with PictureTel endpoints. Select this option for older endpoints. • **Visual Concert PC.** Select this option for use with Polycom ViewStation MP/512/SP/323 endpoints. • **Visual Concert FX.** Select this option for use with Polycom ViewStation FX/EX and VS4000 endpoints. • **Duo Video.** This setting supports IP and ISDN and is available with Tandberg endpoints, in which one part of the conference is set as the video conference and the other as the presentation conference. **Note** The MCU requires that conferences with People + Content use a minimum speed of 192 K.

Setting	Description
T.120 Mode	Selects the protocols and specifications for multipoint data communication. In the **T.120** menu, select the speed for the T.120 connection. See your IT department to determine the best combinations for your conferences. To disable the T.120 mode, select **None**. If you select T.120, these options may be available, according to the participant's endpoint and software: • **Application Sharing.** Allows two or more participants to work on the same document or application, even when only one participant has the application. In application sharing, one participant launches the application, and it runs simultaneously on all other computers. • **File Transfer.** Enables participants to send files to each other. • **Chat or Whiteboard.** Allows participants to communicate with each other by writing. In all of these modes, participants can view and hear each other. **Note** This setting applies to MGC-hosted conferences only.

3 Continuing adding or editing the conference, as described in "Conference Management Operations" on page 31.

Select a Bridge for a Conference

By default when you add a conference, the Polycom CMA system will automatically select a bridge for the conference. However, if you have advanced scheduler permissions, you can select a specific bridge for your conferences.

To selecte a single bridge for a conference

1 On the **Conference Resources** page as you are adding or editing a conference, make a template selection and edit the conference settings, as required.

2 In the **Bridge Selection** menu, select **Single Bridge**.

A bridge selection menu appears based on the template selection and conference settings.

3 In the MCU list, select a specific MCU to host the conference.

4 Continuing adding or editing the conference, as described in "Conference Management Operations" on page 31.

Create a Cascaded Conference Across Multiple Bridges

To create a cascaded conference across multiple bridges

1 When you're adding or editing a conference, after you've made all of your other conference configuration choices, click **Bridge Selection** and select **Multi Bridge**.

The **Schedule** button changes to a **Manual Cascade** button and the **Recurrence** button disappears.

2 Click **Manual Cascade**.

The **People To Bridges** dialog box appears displaying the selected conference participants and their bridge assignments. Bridge assignments default to **Auto**. These system assignments are based on bridge capacity and/or least cost routing principles.

In the **Selected Bridge Availability** section, the system shows a count of the available ports on the available bridges for the specified time period. If the port count is within 5% of the maximum ports available, it is displayed in red.

3 To change a bridge assignment for a selected participant, click **Auto** and select a bridge from the pull-down menu.

Note
A Polycom CMA system can only show port counts for conferences scheduled via the system. Adhoc conferences are not included in the port count.

4 When you've completed all bridge assignments, click **Next**.

The **Bridge To Bridge Links** dialog box displays a graphical view of the selected bridges.

Note
If an MCU does not show up in the **Bridge To Bridge Links** dialog box, then the MCU software does not support cascading.

5 To add a hub bridge (a bridge used to connect one bridge to another), from the **Available Bridges** window, select a bridge and click **Add Bridge**.

6 Specify bridge-to-bridge connections by selecting the bridges of interest and clicking **Add Link**.

The link is graphically represented by an arrow. The bridge at the base of the arrow dials to the bridge at the point of the arrow.

Note

A Polycom RMX system cannot dial a Polycom MGC, so do not link from an RMX to an MGC.

7 In the **Add Link** dialog box, select the **Link Type**.

Notes

- You can add links from a Polycom MGC MCU to a Polycom RMX MCU
- There is no support for ISDN cascaded links on RMX MCUs.
- The lag time required to update cascaded links may cause more than one participant to hear the prompt about being the first person to join the conference.

8 When finished, click **Schedule**.

The system verifies that it has a bridge with the capabilities and resources required for your conference. If it does, the **Conference Email Notification** page appears with a message indicating **Conference Successfully Scheduled**.

9 To exit without sending an email to your participants, click **Skip Email**.

10 To send an email notification to your participants, in the **Conference Email Notification** page:

a Copy additional people on the notification and/or add notes about the conference.

b Click **Send**.

Note that the **To**, **CC**, and **BCC** fields are ASCII only. For more information, see "Field Input Requirements" on page 6.

The system sends the conference notification email. The **Conference List - Schedule View** appears. Your conference appears in the **Conference List**.

Notes

- Recurring cascaded conferences are not allowed.
- You cannot change the conference layout of a cascaded conference.

6

Conference and Participant Details

This chapter lists the conference and participant detail fields for reference. It includes these sections:

Conference Details

The **Conference Details** section has these fields.

Section	Description
Owner	The name of the person who created the conference. Schedulers only see the conferences they own. Not applicable for ad hoc conferences.
Start Date/Time	For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time. For an unscheduled conference, the date and time the conference started.
Duration	For a scheduled conference, how long the conference is scheduled to last. For a completed conference, how long the conference actually lasted.
End Date/Time	The date and time the conference ended

Section	Description
Type	The type of conference. Possible values include: • Audio • Audio-Video
Status	The state of the conference. Possible values include: • Active • Declined • Finished • Future
Recurring	Whether or not the conference was scheduled as a recurring conference
Connection	Connection information about the conference. Possible values include: • Multipoint • Point To Point • Gateway
Bit Rate	The rate (in kbps) at which to transfer the conference audio or video data
Schedule ID	System-assigned ID used for troubleshooting
Conf Monitoring ID	System-assigned ID used for troubleshooting
Video Layout	The video layout for the conference: Continuous Presence or video Switching.
Video Format	For a conference hosted on an MCU, the video format of the conference data stream. Possible values include: • Auto • CIF • QCIF • 4CIF • 16CIF • VGA • SVGA • XGA • NTSC
Video Protocol	For a conference hosted on an MCU, the video protocol of the conference data stream. Possible values include: • Auto • H.261 • H.263 • H.264
Audio Algorithm	For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are: • AUTO • G.711 • G.722 • Siren 7 (16 kbps)

Conference Features

The **Conference Features** section has these fields.

Section	Description
Conference Password	The conference password, which is assigned either by the system or the scheduler
Chairperson Required	Whether or not the conference requires a chairperson **Note** The RMX 1000 system does not support the **Chairperson** feature.
Chairperson Password	The password the chairperson must enter. Not applicable when no chairperson is designated.
Chairperson	The name of the chairperson. Not applicable when no chairperson is designated.
Lecture Mode	The type of **Lecture Mode**, if any, that was selected when the conference was created. Possible values are None and Presentation. **Note** The RMX 1000 system does not support **Lecture Mode**.
Lecturer	The name of the lecturer. Not applicable when **Lecture Mode** is **None**.
Lecture View Switching	Indicates whether or not automatic switching between participants is enabled
Dual Stream Mode	Possible values are: • None • People+Content • Duo Video • Visual Concert PC • Visual Concert FX • Unknown
T120 Rate	Possible values are: • None • HMLP - Var • HMLP - 384 • HMLP - 320 • HMLP - 256 • HMLP - 192 • HMLP - 128 • HMLP - 6.4 • HMLP - 62.4 • HMLP - 14.4 • MLP - Var • MLP - 64.4 • MLP - 62.4 • MLP - 46.4 • MLP - 40 • MLP - 38.4 • MLP - 32 • MLP - 30.4 • MLP - 24 • MLP - 22.4 • MLP - 16 • MLP - 14.4 • MLP - 6.4 • MLP - 4

Section	Description
End Time Alert	Whether or not the system alerts participants to the end of the conference by playing an end tone
Entry Tone	Whether or not an entry tone is played to all connected participants when a participant joins the conference
Exit Tone	Whether or not an exit tone is played to all connected participants when a participant disconnects from the conference

Bridge (MCU) Features

The **Bridge (MCU) Features** section, which applies only for conferences that use an MCU, has these fields.

Section	Description
MCU Name	The MCU device name hosting the conference. Not applicable when the conference is not being hosted on an MCU.
Numeric ID	The unique conference identifier assigned by the MCU
Entry Queue Access	Whether or not the conference has an entry queue enabled **Note** The Polycom CMA system enables entry queues on a per MGC basis and all conferences on an entry queue enabled MGC will be scheduled with entry queue access.
Meet Me per Conf	Whether or not the a conference is a Meet Me conference, for which a dial-in number is assigned, so that undefined participants can connect to the conference
Conference on Port	(MGC only) Indicates whether or not the MGC is set to Conference on Port, which conserves bandwidth and ports. In this case, all participants are on a single video port and use the same connection speed and video format.
Message Service Type	Displays the type of messages participants joining the conference hear. Possible values are: • None • Welcome (No wait) • Attended (Wait) • IVR
Message Service Name	Name on the MCU of the Message Service. So, for example, a service name IVR70 which provides the IVR service

Participants

The **Participants** section has these fields.

Section	Description
Name	The participant's name
Call Info	How the participant joined the call. Possible values include: • Video Dial-Out • Audio Dial-In@<*Address*> • Video Dial-In@<*Address*> • In Person • Room Only

Participant Details

The **Participant Details** section has these fields.

Section	Description
Call Info	How the participant joined the call. Possible values include: • Video Dial-Out • Audio Dial-In@<*Address*> • Video Dial-In@<*Address*> • In Person • Room Only
Video Protocol	For a conference hosted on an MCU, the video protocol of the conference data stream. Possible values include: • Auto • H.261 • H.263 • H.264
Video Format	For a conference hosted on an MCU, the video format of the conference data stream. Possible values include: • Auto • CIF • QCIF • 4CIF • 16CIF • VGA • SVGA • XGA • NTSC

Section	Description
Audio Algorithm	For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are: • Siren 7 (16 kbps) • Siren 14 (24 kbps) • Siren 14 (32 kbps) • Siren 14 (48 kbps) • AUTO • G.711 • G.722
Local Date/Time	The date and time the conference started in local time.
Call ID	System-assigned ID used for troubleshooting.
Callee Name	The names of the participants called
Callee Device	The names of the devices for the called participants
Callee Site	The names of the sites for the called participants
Callee Device Status	The state of the participant's connection. Possible states include: • Connected • Disconnected • Help request • Updating • New dial-in participant • New dial-out participant
Caller Name	The name of the participant who placed the call
Caller Device	The name of the device from which the participant placed the call
Caller Site	The name of the site from which the participant placed the call
Content	None

Section	Description
T120 Rate	Possible values include: • None • HMLP - Var • HMLP - 384 • HMLP - 320 • HMLP - 256 • HMLP - 192 • HMLP - 128 • HMLP - 6.4 • HMLP - 62.4 • HMLP - 14.4 • MLP - Var • MLP - 64.4 • MLP - 62.4 • MLP - 46.4 • MLP - 40 • MLP - 38.4 • MLP - 32 • MLP - 30.4 • MLP - 24 • MLP - 22.4 • MLP - 16 • MLP - 14.4 • MLP - 6.4 • MLP - 4

Participant Settings

The **Participant Settings** dialog box has these fields.

Section	Description
Name	The participant's name
Devices	The participant's managed device(s) if available
Email	The participant's email address (ASCII only[a]) for participants or guests without managed devices
Type	The type of participant. Possible values include: • Domain User • Local User • Domain Resource (a room) • Local Resource (a room) • Guest
How will this participant join the conference?	How the participant will join the conference. Possible values include: • In Person (requires no dial settings) • Room Only • Audio Only (Dial in) • Use Video

Section	Description
Bit Rate	The audio or video data transfer rate (in kbps) of the participant's endpoint
Dial Options	Available only if the participant is joining via a video endpoint system. Possible values include: • Dial-In • Dial-Out
Dial Type	The protocol the audio or video endpoint system uses.

a. For more information on field limitations, see "Field Input Requirements" on page 1-6.

If you select a **Dial Option** of **Dial-Out** for a participant without a managed endpoint, the **Participant Settings** dialog box has these additional fields.

Section	Description
Country	(H.320 dial type only) The country to which the system will dial out to the participant
Area/City Code	(H.320 dial type only) The area code to which the system will dial out to the participant
Number	(H.323 and H.320 dial types) The participant's phone number
Use Modified Dial Number	(H.320 dial type only) Click this check box to add a specific prefix to the participant's phone number. The Number field becomes active
Number	(H.320 dial type only) The complete modified dial number as required to include PBX exit codes, dialing prefixes, or other installation-specific dial string requirements.

7

Endpoint Management Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) system's endpoint management functions. It includes these topics:

Endpoint Types

The following table describes the Polycom CMA system support for endpoints based on endpoint type and type of support.

Endpoint Type	Comments
Full support in dynamic management mode—Gatekeeper registration, monitoring, command and control, automatic provisioning, automatic softupdate, and presence	
Polycom CMA Desktop	Version 1.0 or greater
Polycom HDX Series	Polycom HDX systems version 2.5
Note Endpoint system in dynamic management mode do not automatically register to the Global Address Book.	

Endpoint Type	Comments
Full support in standard/traditional management mode—Gatekeeper registration, Global Address Book registration, monitoring, command and control, scheduled provisioning, and scheduled softupdate	
Polycom HDX Series	Polycom HDX systems version 1.0 through 2.5 operating in standard/traditional management mode
ViewStation	None
ViewStation FX and EX	None
V and VSX Series	None
Limited support in standard/traditional management mode—Gatekeeper registration, Global Address Book registration, management (add, edit, and delete), and limited scheduling (dial-in only)	
Polycom QDX Series	Polycom QDX systems version 3.0 or greater operating in standard/traditional management mode
Limited support in standard/traditional management mode—Gatekeeper registration, Global Address Book registration, and link to management	
Tandberg	The Polycom CMA system supports gatekeeper and GAB registration, scheduled provisioning and scheduled softupdate of key fields (not all fields) on Tandberg MXP Series endpoints, version NTSC including the 990, 880 and 770.
Limited support in standard/traditional management mode—Gatekeeper registration and Global Address Book registration only	
iPower	iPower support is being phased out
PVX	None
Tandberg	The Polycom CMA system supports gatekeeper and GAB registration on Tandberg 6000, Edge95, 1700, 1500 endpoints
Third party support—Gatekeeper registration only	
Sony PCS Version 03.00	None
Aethra Maia Starr Version 5.1.35	None
VCON (Galaxy and Vigo) Version 0202.M05.D28.H12	None
VTEL, all versions	None

A Polycom CMA system may also list an endpoint type of **Other**. The Polycom CMA system cannot control endpoints with a type of **Other** and cannot direct these endpoints to initiate point-to-point calls. A scheduled point-to-point call between two endpoint systems with an endpoint type of **Other** requires the use of an MCU.

Endpoint Menu, Views, and Lists

The Polycom CMA system **Endpoint** menu provides these views of the **Endpoint** list:

- **Monitor View**—Displays the list of all registered endpoints. Use this view to manage endpoints. See "Monitor View" on page 64.
- **Automatic Provisioning**—Displays the list of dynamically managed endpoints eligible for automatic provisioning. See "Automatic Provisioning View" on page 66.
- **Scheduled Provisioning**—Displays the list of traditionally managed endpoints eligible for scheduled provisioning. See "Scheduled Provisioning View" on page 67.
- **Automatic Softupdate**—Displays the list of dynamically managed endpoints eligible for automatic software updates. See "Automatic Softupdate View" on page 69.
- **Scheduled Softupdate**—Displays the list of traditionally managed endpoints eligible for scheduled software updates. See "Scheduled Softupdate View" on page 70.

All of the **Endpoint** views have the following information:

Section	Description
Views	The views you can access from the page
Actions	The set of available commands. The constant command in the **Endpoint** views is **Refresh**  , which updates the display with current information.
Endpoint List	The context-sensitive **Endpoint** list for the selected view
Device Details	Information about the endpoint selected in the endpoint list including: • "Device Summary Information" on page 131 • "Device Status Information" on page 133 • "Call Information" on page 135 • "Device Alerts Information" on page 136 • "Provisioning Details" on page 136 • "Softupdate Details" on page 137

Monitor View

Use the **Endpoint Monitor View** to monitor and manage endpoints.

Endpoint List in the Monitor View

By default the **Endpoint** list in the **Monitor View** displays a comprehensive list of all endpoints managed by the Polycom CMA system, including endpoints that registered automatically with the Polycom CMA system and endpoints that were added manually for management and monitoring purposes.

The **Endpoint** list in this view has these fields.

Field	Description
Filter	Use the filter choices to display other views of the **Endpoint** list, which include: • **Type**- Filters the list by type. For more information, see "Endpoint Configuration/Provisioning" on page 71. • **Alerts**- Filters the list by alert type: Help, Error, or Warning • **Connection Status**- Filters the list by connection status: In a Call, Online, or Offline • **Name** - Filters the list by system name entered • **IP Address** - Filters the list by IP address entered • **ISDN Video Number** - Filters the list by ISDN video number entered • **Alias** - Filters the list by the alias entered • **Site** - Filters the list by site location entered • **VIP** - Filters the list for VIP endpoints
Status	The state of the endpoint. Possible values include: • Online • Offline • In a call • Unknown • Device alert • Gatekeeper registration error
Mode	The management mode for the endpoint. Possible values include: • Dynamic management mode • Traditional management mode (no icon) For a description of these modes, see "Endpoint Configuration/Provisioning" on page 71.
Name	The assigned name of the endpoint

Field	Description
Type	The type of endpoint. For valid endpoint types, see "Endpoint Configuration/Provisioning" on page 71.
IP Address	The IP address assigned to the endpoint
Alias	The alias assigned to the endpoint
Site	The site to which the endpoint belongs
Owner	The user associated with the endpoint

Commands in the Monitor View

Besides providing access to the endpoint views, the **Actions** section of the **Monitor View** may also include these context-sensitive commands depending on the selected endpoint type.

Command	Use this command to ...
Available for all endpoint types	
Add 	Manually add an endpoint to the Polycom CMA system or find a endpoint on the network
View Details 	Display all of the **Device Details** for the selected endpoint
Edit 	Change connection settings for the selected endpoint. Note that if this is a managed endpoint, the endpoint may overwrite settings entered manually.
Delete 	Delete the selected endpoints
Available for only selected endpoint types	
Manage 	Open the selected endpoint's management interface in a separate browser window. This command is not available for the following endpoint types: **iPower**, **PVX**, and **Other**.
Send Message 	Send a text message (ASCII only[a], 100 characters maximum) to the selected endpoint's video monitor. This command is not available for the following endpoint types: **Tandberg**, **iPower**, and **Other**.
Clear Help 	Clear help for the selected endpoint on the Polycom CMA system
Reboot Device 	Reboot the selected endpoint. This command is only available for **HDX-Series**, **V-Series** and **VSX-Series** endpoints with a **Connection Status** of **Online**.

Command	Use this command to ...
Manage User	Change information for the selected user. This command is applicable only when the user is associated with a endpoint.

a. For more information on field limitations, see "Field Input Requirements" on page 6.

For information about these endpoint commands, see "Endpoint Management Operations" on page 95.

Automatic Provisioning View

Use the **Automatic Provisioning View** to see the list of endpoints that are registered to the system for automatic provisioning.

Endpoint List in the Automatic Provisioning View

By default the endpoint list in the **Automatic Provisioning View** displays the list of Polycom HDX system endpoints registered to the Polycom CMA system for automatic provisioning.

The endpoint list in the **Automatic Provisioning View** has the following information.

Field	Description
Filter	The filter choice for endpoint types that can be automatically provisioned. Possible values include: • HDX Series—Displays just the Polycom HDX systems deployed in dynamic management mode • CMA Desktop—Displays just the Polycom CMA systems • All—Displays the Polycom HDX systems deployed in dynamic management mode and Polycom CMA Desktop systems together
Status	The status of the endpoint's last provisioning process. Possible values include: • Success • Failed • Clear
Name	The assigned name of the endpoint **Note** The system assigns Polycom CMA Desktop systems a user name of LastName_Firstname_CMADesktop.

Field	Description
Type	The type of endpoint. Automatic provisioning is only available for these endpoint types: • HDX Series--Polycom HDX system endpoints deployed in dynamic management mode • CMA Desktop—Polycom CMA Desktop systems
IP Address	The IP address assigned to the endpoint
Last	The date and time of the endpoint's last provisioning **Note** Polycom CMA Desktop systems are provisioned at the start of each session.

Commands in the Automatic Provisioning View

Because automatic provisioning is managed by the endpoint, there are no context-sensitive commands available in the **Automatic Provisioning View**.

Scheduled Provisioning View

Use the **Scheduled Provisioning View** to:

- View the list of endpoints that are eligible for scheduled provisioning
- Schedule one or more endpoints for provisioning
- Cancel a scheduled provisioning

Endpoint List in the Scheduled Provisioning View

By default the endpoint list in the **Scheduled Provisioning View** displays the list of Polycom HDX system endpoints registered to the Polycom CMA system that are eligible for scheduled provisioning.

The **Endpoint** list in this view has the following information.

Field	Description
Filter	The filter choice for endpoint types that can be scheduled for provisioning. Possible values include: • HDX Series—Displays the Polycom HDX systems operating in standard/traditional management mode • V and VSX Series • Viewstation • Viewstation FX & EX • Tandberg

Field	Description
Status	The status of the endpoint's last provisioning process. Possible values include: • Success • Failed • Pending • Clear
Name	The system name of the endpoint
Type	The type of endpoint. Scheduled provisioning is only available for the endpoints types listed previously as Filter selections.
IP Address	The IP address assigned to the endpoint
Last	The date and time of the endpoint's last provisioning, unless its status has been cleared
Pending	When the endpoint is scheduled for provisioning, this field shows the provisioning profile to be used for the scheduled provisioning process
Scheduled	When the endpoint is scheduled for provisioning, this field shows the date and time for the next scheduled provisioning process

Commands in the Scheduled Provisioning View

Besides providing access to the endpoint views, the **Commands** section of the **Scheduled Provisioning View** also includes these commands:

Command	Use this command to ...
Provision 	Schedule provisioning for the selected endpoint(s).
Cancel Provision 	Cancel a previously scheduled provisioning operation.
Clear Status 	Change the status column for a endpoint to the **Clear** state

You can perform these operations on multiple endpoints at the same time. To select multiple endpoints, hold the control key while you select the endpoints.

For information about these endpoint commands, see "Endpoint Provisioning Operations" on page 107.

Automatic Softupdate View

Use the **Automatic Softupdate View**, available from the **Endpoint** menu, to view the list of endpoints that have registered to the system for automatic (pull) softupdates.

Endpoint List in the Automatic Softupdate View

By default the **Endpoint** list in the **Automatic Softupdate View** displays all endpoints eligible for automatic softupdate. It has the following information.

Field	Description
Filter	Filter choices for this view include: • **Type**—Filters the list by endpoint type • **Name**—Searches the list by the endpoint's system name • **IP Address**—Searches the endpoint list by IP address • **ISDN Video Number**—Searches the endpoint list by ISDN video number • **Alias**—Searches the endpoint list by alias • **Site**—Searches the endpoint list by site location
Status	The status of the endpoint's last softupdate. Possible values include: • Success • Failed • Clear
Name	The system name of the endpoint
Type	The type of endpoint. Automatic softupdate is only available for these endpoint types: • HDX Series—Polycom HDX systems deployed in dynamic management mode • CMA Desktop—Polycom CMA Desktop systems
IP Address	The IP address assigned to the endpoint
Current Version	The version of software installed during the last successful softupdate procedure

Commands in the Automatic Softupdate View

Because automatic (pull) softupdate is managed by the endpoint, there are no commands available in the **Automatic Softupdate View**.

Scheduled Softupdate View

Use the **Scheduled Softupdate View**, available from the **Endpoint** menu, to:

- View the list of endpoints that are eligible for a scheduled softupdate
- Schedule one or more endpoints for a softupdate
- Cancel a softupdate.

Endpoint List in the Scheduled Softupdate View

By default the **Endpoint** list in the **Scheduled Softupdate View** displays all endpoints eligible for scheduled softupdate.

The **Endpoint** list in the **Scheduled Softupdate View** has the following information.

Field	Description
Filter	Filter choices for this view include: • **Type**—Filters the list by endpoint type • **Name**—Searches the list by the endpoint's system name • **IP Address**—Searches the list by endpoint's IP address • **ISDN Video Number**—Searches the list by endpoint's ISDN video number • **Alias**—Searches the list by endpoint's alias • **Site**—Searches the list by site location
Status	The status of the endpoint's last scheduled softupdate. Possible values include: • Success • Failed • Clear
Name	The system name of the endpoint
Type	The type of endpoint. Scheduled softupdate is only available for these endpoint types: • HDX Series--Polycom HDX systems operating in standard/traditional management mode • V and VSX Series • ViewStation FX and EX • ViewStation • Tandberg

Field	Description
IP Address	The IP address assigned to the endpoint
Current Version	The version of software installed during the last successful softupdate procedure
Scheduled	When the endpoint is scheduled for softupdate, this field shows the date and time for the scheduled softupdate process

Scheduled Softupdate View Commands

Besides providing access to the endpoint views, the **Command** section for the **Scheduled Softupdate View** will also include these commands:

Command	Use this command to ...
Software Update 	Schedule softupdate for the selected endpoints
Cancel Update 	Cancel a previously scheduled softupdate operation. You cannot cancel a softupdate once it has started.
Clear Status 	Change the status column for an endpoint to the **Clear** state

For information about these endpoint commands, see "Endpoint Softupdate Operations" on page 115.

Endpoint Configuration/Provisioning

The Polycom CMA system device provisioning, which requries provisioning profiles, allows an administrator to configure one or more devices with a standard set of information the registering devices need to operate within the network. This eliminates the need to configure each device individually.

The Polycom CMA system supports two exclusive types of device provisioning: automatic and scheduled. Automatic and scheduled device provisioning are exclusive management scenarios. Devices enabled for automatic provisioning should not be scheduled for provisioning through the Polycom CMA system.

Note

Polycom recommends that all endpoints in a region (i.e., a gatekeeper zone) be managed by a single management system.

For more information, see:

- Automatic Device Provisioning
- Scheduled Device Provisioning

Automatic Device Provisioning

The Polycom CMA system is a gatekeeper; it manages video and audio devices. However, the system also manages users, because devices are only useful when they provide access to users.

Automatic device provisioning, which controls the automatic configuration of devices and the management of video resources, is also tied to users and groups. That's because some users and groups may require significantly more video resources than others.

Currently, automatic device provisioning is only available for:

- Polycom HDX systems deployed in dynamic management mode
- Polycom CMA Desktop clients

Note
Polycom CMA Desktop provisioning occurs on a session by session basis.

How Automatic Device Provisioning Works

In dynamic management mode, when a device starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the Polycom CMA system. The provisioning information is sent in XML format over a secure HTTPS connection.

Devices do not poll for provisioning information if they are in a call. They restart polling after the call ends.

Automatic Provisioning Profiles

Automatic device provisioning is enabled at the device, but the Polycom CMA system must have automatic provisioning profiles for both the device and the site at which the device resides. So to ensure out-of-box usability, the Polycom CMA system comes with default automatic provisioning profiles for both. However, you can edit these default profiles to meet your needs or add additional provisioning profiles to assign different video resources to different groups of users.

The following table show the fields you can define when adding a new automatic provisioning profile. You may find more implementation details about these fields in the endpoint system documentation.

Field	For the endpoint systems being provisioned...
System Settings	
Language	Specifies the language for the video endpoint system's user interface. Possible values include: English, German, Spanish, French, and Chinese (Simplified Chinese only).
Allow Access to User Setup	Specifies whether the **User Settings** screen is accessible to users via the **System** screen. Select this option if you want to allow endpoint system users to change limited environmental settings.
Allow Directory Changes	Specifies whether endpoint system users can save changes they make to the directory on contacts list.
Call Detail Report	Specifies whether to collect call data for the **Call Detail Report** and **Recent Calls** list. When selected, information about calls can be viewed through the endpoint system's web interface and downloaded as a `.csv` file. **Note** If this setting is disabled, applications such as the Polycom CMA system or the Polycom Global Management System™ will not be able to retrieve Call Detail Report (CDR) records.
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.
Recent Calls	Specifies whether to display the **Recent Calls** button on the home screen. The **Recent Calls** screen lists the site number or name, the date and time, and whether the call was incoming or outgoing. **Note** If the **Call Detail Report** option is not selected, the **Recent Calls** option is not available.
Screen Saver Wait Time	Specifies how long the system remains awake during periods of inactivity. The default is 3 minutes. If the system requires users to log in, the screen saver timeout also logs out the current user. Setting this option to **Off** prevents the system from going to sleep. To prevent image burn-in, specify 3 minutes or less.
Home Screen Settings	
Display Contact List as Home Screen	Specifies whether or not to display the contact list as the entry screen.

Field	For the endpoint systems being provisioned...
Display H.323 Extension	Lets users placing a gateway call enter the H.323 extension separately from the gateway ID. If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format: `gateway ID + ## + extension`
Enable Availability Control	When enabled, lets users set their availability in the endpoint system's local user interface.
H.323 Settings	
Maximum Speed for Receiving Calls (kbps)	Allows you to restrict the bandwidth used when receiving calls. If the far site attempts to call the endpoint system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.
Preferred Speed for Placing Calls (kbps)	Determines the speeds that will be used for calls from this endpoint system when: • The **Call Quality** selection is either unavailable or set to **Auto** on the **Place a Call** screen • The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.
Call Settings	
Preferred Dialing Method	Specifies the preferred method for dialing various call types. • If set to **Auto**, calls use the configured dialing order. • If set to **Manual**, the endpoint systems will prompt the user to select the call type from a list when placing a call.
Audio Settings	
Mute Auto Answer Calls	Specifies whether or not to automatically mute incoming calls.
CMA Desktop Settings	
Allow IM/Chat	When enabled, specifies that the Polycom CMA Desktop client can initiate instant messaging.
Answer Only	When enabled, specifies that the Polycom CMA Desktop client can answer incoming instant messages.

Profile Order and Priority

Automatic provisioning profiles are associated with groups, but what about those users who belong to more than one group—what determines their experience? When you add new profiles, you assign a **Profile Order**. The **Profile Order** determines which provisioning profile takes priority.

Consider the following example:

- Jason Smith is part of the Support group and also part of the Executive group.
- The Support group is assigned an automatic provisioning profile named Low-Bandwidth, which allows a maximum speed for receiving calls of 128kbps.
- The Executive group is assigned an automatic provisioning profile called High-Bandwidth, which allows a maximum speed for receiving calls of 1920kbps
- The Low-Bandwidth profile is assigned a profile order of 1, while the High-Bandwith profile is assigned a profile order of 2.

In this example, Jason's device is provisioned with the Low-Bandwidth provisioning profile, because it has the higher priority.

So when you add provisioning profiles, you may want to assign provisioning profiles with more robust privileges a higher priority than those providing less privileges.

Scheduled Device Provisioning

Scheduled device provisioning is enabled at the Polycom CMA system. To schedule a device for provisioning, the Polycom CMA system must already have a scheduled provisioning profile created for the device.

How Scheduled Device Provisioning Works

In this standard/traditional management mode, administrators with **System Setup** permissions can schedule provisioning for one device or a group of devices; and they can schedule provisioning to occur immediately or for a date and time in the future. The provisioning data is sent in XML format over a secure HTTPS connection.

Scheduled provisioning is available for these device types:

- ViewStation endpoints
- ViewStation FX & EX endpoints
- V and VSX Series endpoints
- Tandberg endpoints

- HDX Series--Polycom HDX systems deployed in standard/traditional management mode

Scheduled Provisioning Profiles

The Polycom CMA system does not include a default profile for scheduled provisioning. You must create a profile before you can schedule a device for provisioning. Create a different profile for each device type (Polycom HDX system or Polycom CMA Desktop) and group of users.

Some examples of when to use scheduled provisioning profiles follow.

- To apply a standard set of options to each new device

  By creating templates of standard settings for different types of devices, or for the needs of different users, you can have the Polycom CMA system apply all the settings at once. After the device is connected and registered with the Polycom CMA system, you can use a provisioning profile that defines a range of other options.

- To update the password for all devices of a particular type

  For security purposes, you can create a provisioning profile to update the password for endpoints on a regular basis and reuse the same profile quarterly. You might have several profiles, one for each type of device you want to update.

- To change the IP address of the Polycom CMA system gatekeeper when the Polycom CMA system is moved

Scheduled Provisioing

The following table show the fields you can define when adding a new scheduled provisioning profile for a .

Field	For the endpoint systems being provisioned...
General Settings	
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.
Allow Mixed IP and ISDN calls	Specifies whether users can make multipoint calls that include both IP and H.320 sites.
Auto Answer Point-to-Point Calls	Specifies whether to answer incoming point-to-point calls automatically.
Auto Answer Multipoint Calls	Specifies whether to answer incoming multipoint calls automatically.
Allow Directory Changes	Specifies whether users can save changes to the directory or Contacts list.
Confirm Directory Additions	Specifies whether users are prompted to confirm deletions of directory entries.
Confirm Directory Deletions	Specifies whether users are prompted to confirm new directory entries when saving the information for the last site called.
Allow Access to User Setup	Specifies whether the User Settings screen is accessible to users via the System screen. Select this option if you want to allow users to change limited environmental settings.
Video Network > IP Network > H.323 Settings	
Enable IP H.323	Allows the system to make IP calls
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far sites you will call. If callers experience issues when sharing content with other Polycom systems, disable this setting.
Transcoding	Specifies whether the system allows each far-site system to connect at the best possible call rate and audio/video algorithm. If transcoding is disabled, the Polycom HDX system down-speeds all connections to the same call rate.
Video Network > IP Network > Gatekeeper	

Field	For the endpoint systems being provisioned...
Use Gatekeeper	Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **Off** — Calls do not use a gatekeeper. • **Auto** — System attempts to automatically find an available gatekeeper. • **Specify** — Calls use the specified gatekeeper. Enter the gatekeeper's IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13).
Gatekeeper IP Address	If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper's IP address. If you chose to specify a gatekeeper, enter the IP address.
Outbound Call Route	Choices: • Gateway • ISDN
Use Gatekeeper for Multipoint Calls	Specify whether multipoint calls use the system's internal multipoint capability or the Conference on Demand feature.
Video Network > IP Network > Gateway Number	
Country Code	Specifies the country code for the system's location
Area Code	Specifies the area or city code for the system's location
Gateway Number	Specifies the gateway's number
Gateway Number Type	Specifies the number type users enter to call this system: • Direct Inward Dial — Users enter an internal extension to call this system directly. **Note** If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias. • Number + Extension — Users enter the gateway number and the system's extension to call this system.
Number of digits in DID Number	Specifies the number of digits in the DID number. The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits.

Field	For the endpoint systems being provisioned...
Number of digits in Extension	Specifies the number of digits in the extension used when Direct Inward Dial is selected. Your organization's dial plan determines this number.
Video Network > IP Network > Gateway Setup	
Speed	Enter a prefix or suffix for each bandwidth you want to allow for gateway calls. Associating prefixes and suffixes with particular bandwidths on your gateway can optimize the use of bandwidth by your organization. Be sure the gateway is configured to use the same prefixes and suffixes you define for the system.
Prefix	
Suffix	

Field	For the endpoint systems being provisioned...
Video Network > IP Network > Quality of Service Settings	
Type of Service	Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedenc**e — Represents the priority of IP packets sent to the system. The value can be between 0 and 5. • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.
Type of Service Value	Specifies the IP Precedence or Diffserv value for Video, Audio, and Control.
Video Type of Service Value	Specifies the IP Precedence or Diffserv value for video packets.
Audio Type of Service Value	Specifies the IP Precedence or Diffserv value for audio packets.
FECC Type of Service Value	Specifies the IP Precedence or Diffserv value for Far End Camera Control packets.
Enable Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum line speed for a call
Enable PVEC	Allows the system to use PVEC (Polycom Video ErrorConcealment) if packet loss occurs.
Video Network > IP Network > Firewall Settings	
Use Fixed Ports	Specifies whether to define the TCP and UDP ports. • If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. • If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. **Note** You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic.

Field	For the endpoint systems being provisioned...
Start TCP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specifiy. **Note** You must also open the firewall's TCP port 1720 to allow H.323 traffic.
Start UDP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specifiy.
NAT Configuration	Specifies whether the endpoint systems should determine the NAT Public WAN Address automatically. • If the endpoint systems are behind a NAT that allows HTTP traffic, select **Auto**. • If the endpoint systems are behind a NAT that does not allow HTTP traffic, select **Manual**. Then specify a **NAT Public (WAN) Address**. • If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select **Off**.
NAT Public (WAN) Address	When **NAT Configuration** is set to **Manual**, specifies the address that callers from outside the LAN should use to call the endpoint systems.
NAT is H.323 Compatible	Specifies that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.
Address Displayed in Global Directory	Specifies whether or not to include the endpoint system's information in the global directory
Video Network > ISDN BRI Protocol	
Enable ISDN H.320	Allows this system to make H.320 (ISDN) calls.
Number of ISDN Channels to Dial in Parallel	Specifies how many channels to dial at one time. You can specify up to eight channels. If you experience network problems, decrease the number. Set this value to 1 for serial dialing. Serial dialing is not recommended unless you have trouble connecting calls using parallel dialing.
ISDN Switch Protocols	Specifies the protocol used by your network's switch.
Outside Line Dialing Prefix	Specifies the ISDN dialing prefix used to call outside the network.

Field	For the endpoint systems being provisioned...
Video Network > Preferred Speeds	
Preferred Speed for Placing Calls (Kbps) IP Calls ISDN Video Call (H.320) International ISDN calls	Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when: • The **Call Quality** selection is either unavailable or set to **Auto** on the **Place a Call** screen • The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.
Maximum Speed for Receiving Calls (Kbps) IP Calls ISDN Video Call (H.320)	Allows you to restrict the bandwidth used when receiving IP or ISDN calls. If the far site attempts to call the system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.
Monitors	
Monitor 1 Options	
Monitor 1	Specifies the monitor's aspect ratio. • 4:3 — Select if you are using a regular TV monitor.
Video Format	Specifies the monitor's format: • DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. • VGA — Select if the monitor is connected to the DVI connector using a VGA cable. • Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors. • S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. • Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.
Display Icons in Call	Specifies whether to display all on-screen graphics, including icons and help text, during calls.
Snapshot Timeout	Lets you choose whether to have slides and snapshots time out after a period of four minutes.
Dual Monitor Emulation	Specifies whether the system can show multiple views on a single display.

Field	For the endpoint systems being provisioned...
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates. • Select **Black** if you want to display black video. This is the recommended setting to prevent burn-in for TV monitors. • Select **No Signal** if you want the display to react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors.
Monitor 2 Options	
Monitor 2	Specifies the second monitor's aspect ratio: • Off — Select if you do not have a second monitor. • 4:3 — Select if you are using a regular TV monitor as the second monitor.
Video Format	Specifies the monitor's format: • DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. • VGA — Select if the monitor is connected to the DVI connector using a VGA cable. • Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors. • S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. • Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates. • Select **Black** if you want to display black video. This is the recommended setting to prevent burn-in for TV monitors. • Select **No Signal** if you want the display to react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors.

Field	For the endpoint systems being provisioned...
Monitor 3 Options	
Monitor 3	Specifies the aspect ratio for recording. • Off — Select if you do not have a VCR or DVD player connected to record video conferences. • 4:3 — Select to record for playback on a standard monitor. • 16:9—Select to record for playback on a wide-screen monitor, if your recording device has this capability. See the endpoint product documentation for more information about these selections.
Video Format	Specifies the VCR or DVD player's format: • S-Video — Select if the VCR or DVD player is connected to a Polycom HDX system using an S-Video cable. • Composite — Select if the VCR or DVD player is connected to a Polycom HDX system using a composite video cable and S-Video to RCA adapter.
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the VCR or DVD player when the system goes to sleep and the screen saver activates. • Select **Black** if you want to send black video. • Select **No Signal** if you want the VCR or DVD player to react as if it is not connected when the system goes to sleep.
VCR/DVD Record Source Near Far Content	Specifies the video source to be recorded to videotape or DVD. • If **Far** is enabled, the recorded video will switch to the current far site speaker. • If both **Near** and **Far** are enabled, the recorded video will switch between near and far sites depending on the current speaker. • If **Content** is enabled, any content sent during the call is recorded.
Cameras > Camera 1	
Far Control of Near Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this option is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site.
Backlight Compensation	Specifies whether the camera should automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.

Field	For the endpoint systems being provisioned...
Primary Camera	Specifies which camera is the main camera.
Camera Direction	Specifies the direction the camera moves when using the arrow buttons on the remote control.
Cameras > Camera Settings	
Camera 1 Name	Specifies a name for camera 1.
Camera 1 Icon	Specifies an icon for camera 1.
Camera 2 Name	Specifies a name for camera 2.
Camera 2 Icon	Specifies an icon for camera 2.
Camera 3 Name	Specifies a name for camera 3.
Camera 3 Icon	Specifies an icon for camera 3.
Cameras > Video Quality	
Camera 1 Camera 2 Camera 3	Specifies Motion or Sharpness for the video input. The default is Sharpness. • **Motion** — This setting is for showing people or other video with motion. • **Sharpness** — The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is recommended for HD calls between 1 Mbps and 2 Mbps.
Audio Settings > Audio Settings 1	
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.
Incoming Video Call	Specifies the ring tone used for incoming calls.
User Alert Tones	Specifies the tone used for user alerts.
Mute Auto Answer Calls	Specifies whether to mute incoming calls. Incoming calls are muted by default until you press the mute on the microphone or on the remote control.
Line Input (Red)	Specifies the type of equipment that is connected to audio input 1.
Line Input Level (Red)	Sets the volume level for audio input 1.
Line Input (White)	Specifies the type of equipment that is connected to audio input 2.
Line Input Level (White)	Sets the volume level for audio input 2.

Field	For the endpoint systems being provisioned...
Line Outputs	Specifies how the audio output behaves. The default selection, **Monitor - Far Site Audio**, supplies audio to the Monitor 1 audio outputs only when the system is receiving audio from the far site. If you have connected a VCR to record the conference, select **Monitor - Far and Near Audio** to supply audio from both the far site and the system's microphones.
Line Output Level	Sets the volume level for audio output
Audio Settings > Audio Settings 2	
Master Audio Volume	Sets the volume level for audio from the far site.
Midrange Speakers	Specifies whether to use the system's built-in midrange speaker. You may prefer to turn off the midrange speaker if you connect the audio output to Monitor 1 or if you connect an external speaker system.
Bass	Sets the volume level for the low frequencies without changing the master audio volume.
Treble	Sets the volume level for the high frequencies without changing the master audio volume.
LAN Properties > LAN Properties 1	
Connect to My LAN	Enables connection to the local area network
Host Name	
IP Address	Specifies how the system obtains an IP address. • **Obtain IP Address Automatically** — Select if the system gets an IP address from the DHCP server on the LAN. • **Enter IP Address Manually** — Select if the IP address will not be assigned automatically.
Use the Following IP Address	If you selected **Enter IP Address Manually**, enter the IP address here.
LAN Properties > LAN Properties 2	
DNS Servers	Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. Changing this setting causes the system to restart.
Default Gateway	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.

Field	For the endpoint systems being provisioned...
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.
WINS Server	Displays the server running the Windows Internet Name Service
WINS Resolution	Enables connection to the WINS Server for URL resolution
LAN Speed	Specify the LAN speed to use. Note that the setting you choose must be supported by the switch. Choose Auto to have the network switch negotiate the speed automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets Duplex Mode to Auto. If you choose 10 Mbps, 100 Mbps, or 1000 Mbps you must set Duplex Mode to Half or Full. Changing this setting causes the system to restart.
Duplex Mode	Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose Auto to have the network switch negotiate the Duplex mode automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets LAN Speed to Auto. Changing this setting causes the system to restart.
Global Services > Directory Servers	
Global Directory (GDS)	Specifies the IP address or DNS address of the Global Directory Server.
Password	Lets you enter the global directory password, if there is one.
Display Name in Global Directory	Specifies whether to display the system's name in the global directories of other registered systems.
Display Global Addresses	Displays other registered systems in the global directory.
Register	Registers this system with the Global Directory Server.
Save Global Directory to System	Copies the global directory to this local system. When this setting is disabled, the system can display no more than 1,000 global directory entries. When this setting is enabled, the system can display up to 4,000 global directory entries.

Field	For the endpoint systems being provisioned...
Global Services > Dialing Rules 1	
Number of digits in Extension	Specifies the number of digits in the extension. Your organization's dial plan determines this number.
International Dialing Prefix	Specifies the dialing prefix needed for international calls
Public Network Access	Specifies if calls can be made to the public network
Public Network Dialing Prefix	Specifies the dialing prefix used to call out to endpoints on the public network when the endpoint is not in the same area code as the system
Public Network (same area code) Prefix	Specifies the dialing prefix used to call out to endpoints on the public network when the endpoint is in the same area code as the system
Private Network Dialing Prefix	Specifies the dialing prefix used to call outside the network
Private Network Access	Specifies if calls can be made to the private network
Global Services > Dialing Rules 2	
If Area Code Equals/ Dial Prefix Pairs	Create additional dialing rules and routing based on area code
Always Dial Area Code	Specify whether the phone number must always include an area code
Dial 1+ for all USA Calls	Specify whether to preface calls within the United States with 1
Global Services > Account Validation	
Require Account Number to Dial	Specify whether to require an account number for placing calls and whether that number should be validated by the system.
Validate Account Number	Specify whether to require an account number for placing calls and whether that number should be validated by the system.
Global Services > My Information	
Contact Person	Specifies the name of the person responsible for this system
Contact Number	Specifies the phone number of the person responsible for this system
Contact Email	Specifies the email address of the person responsible for this system
Contact Fax	Specifies the Fax number of the person responsible for this system

Field	For the endpoint systems being provisioned...
Tech Support	Specifies the contact information for Technical Support for this system
City	Specifies the location of the person responsible for this system
State/Province	
Country	

Some notes about scheduled provisioning profiles and the scheduled provisioning of endpoints:

- Each page in the scheduled **Provisioning Field**s dialog box has a **Provision This Page** option. When this option is selected, the system provisions all of the values on that page. When this option is not selected, the system does not provision any of the values on that page. At least one page must be provisioned, or the system returns an error stating, "No data to save in profile. Either press **Cancel** or add pages."
- Until the Polycom CMA system successfully provisions an endpoint scheduled for provisioning, provisioning remains in the **Pending** state and the system attempts to provision the endpoint until it succeeds or until the provisioning is cancelled.
- If an endpoint scheduled for provisioning is **In a Call**, the system waits until the call ends before provisioning the endpoint. The system checks the endpoint at 15 minute intervals.
- If an endpoint scheduled for provisioning is **Offline**, the system attempts to connect to the endpoint at 60 minute intervals until the endpoint is **Online**.
- Provisioning may reboot the endpoint
- You can schedule provisioning for as many endpoints as desired at one time, but the system may limit the number of active provisioning processes

Endpoint Gatekeeper Registration Policies

If the Polycom CMA system gatekeeper registration policy allows endpoints to register automatically (that is, a primary gatekeeper setting of **Allow Registration of All Endpoints**, **Allow Registration of Endpoints in Defined Sites**, or **Allow Registration of Endpoints with Defined E.164 Prefixes**), those registered endpoints are automatically added to the endpoint list.

If the Polycom CMA gatekeeper registration policy does not allow endpoints to register automatically (i.e., a gatekeeper setting of **Allow Registration of Predefined Endpoints Only**), you must manually add all endpoints to the Polycom CMA system.

No matter what the gatekeeper registration policy, any endpoint that is automatically provisioned, any endpoint that is registered with the Global Address Book, and any endpoint that is added manually to the Polycom CMA system can automatically register with the gatekeeper.

Note
You can also manually add endpoints to the Polycom CMA system for monitoring purposes only.

For more information, see "Device Registration" on page 242.

Endpoint Softupdates

The Polycom CMA system softupdate feature, which requires a softupdate profile for the device type and model, allows an administrator to upgrade the software on one or more endpoints with a standard software package. This eliminates the need to upgrade each device individually.

The Polycom CMA system supports two exclusive softupdate processes: automatic and scheduled. Automatic and scheduled softupdate are exclusive endpoint management scenarios. Endpoints enabled for automatic softupdate should not be scheduled for softupdates through the system.

Note
Polycom recommends that all endpoints in a region (i.e., a gatekeeper zone) be managed by a single management system.

For more information, see:

- Automatic Device Softupdates
- Scheduled Device Softupdates

Automatic Device Softupdates

Automatic device softupdate, which controls the device's software version level, is tied to the Device Type. Currently, the automatic softupdate feature is only available for these device types.

- Polycom HDX system endpoints deployed in dynamic management mode
- Polycom CMA Desktop systems

How Automatic Device Softupdate Works

In dynamic management mode, when a device starts up and at designated intervals thereafter, it automatically polls the Polycom CMA system for a newer softupdate package. If a softupdate is necessary, the package is sent in XML format over a secure HTTPS connection.

Devices do not poll for softupdate packages if they are in a call. They restart polling after the call ends.

Automatic Softupdate Profiles

Automatic softupdate is enabled at the device, but the Polycom CMA system must have an automatic softupdate profile for the Device Type to fulfill the process. A default automatic softupdate profile—with the description **CMA Desktop - shipped version**—is available for the Polycom CMA Desktop client. Default automatic softupdate profiles are not available for other endpoint systems. To create an automatic softupdate profile, you upload the software package and create a profile for the update.

Automatic Softupdate Versions

After creating an automatic softupdate profile, you can use the **Version to use** and **Allow this version or newer** selections to manage the roll out of softupdate packages. These selections also allow you to manage the release of multiple software packages for the same device type.

Here's how it works:

All devices have a current version of software. To automatically overwrite that current software with a different software version on all dynamically managed endpoint systems:

1. You first create a new automatic softupdate profile that includes the new softupdate package.
2. Then to activate the roll out, you change the **Version to use** selection from the current value (**None** by default) to the new version number and **Update** the page.

The next time a dynamically managed endpoint polls the Polycom CMA system, it will detect that it has a different software version than the **Version to use** selection, so it will automatically download and install the identified softupdate package. Use this method to force users to use a specific software version.

> **Note**
> Until the **Version to use** selection is enabled, the automatic softupdate is not activated.

If you also enable the **Allow this version or newer** selection, anytime you package a newer version of software into an automatic software profile that package will be automatically installed on all dynamically managed endpoint systems.

Some important things to note about software versions

- Newer software is identified by the version number. If the **Allow this version or newer** selection is enabled, when a dynamically managed endpoint polls the Polycom CMA system, the system will compare the current software version number with the packaged software version numbers. The Polycom CMA system will send the software package with the highest version number to the endpoint.
- You can also use the **Version to use** selection to roll devices back to older software versions. If you change the **Version to use** selection to an older software version and clear the **Allow this version or newer** selection, the Polycom CMA system will send the specifically identified software package to the endpoint even if it is an older version.

Note

Currently to roll back a Polycom CMA Desktop client to an older version, you must first remove the existing Polycom CMA Desktop client via the Windows **Add or Remove Software** selection. Then you can install the older software package.

Scheduled Device Softupdates

The scheduled softupdate feature is enabled at the Polycom CMA system. An administrator with **System Setup** permissions can schedule softupdates for one device or a group of devices to occur immediately or for a date and time in the future.

Scheduled softupdates are available for these device types.

- ViewStation
- ViewStation FX & EX
- V and VSX Series
- Tandberg MXP series
- HDX Series--Polycom HDX system devices operating in standard/traditional management mode

Some notes about scheduled softupdates:

- Until the Polycom CMA system successfully updates an endpoint scheduled for updating, the update remains in the **Pending** or **In Progress** state and the Polycom CMA system attempts to update the endpoint until it succeeds or until the update is cancelled.

- If an endpoint scheduled for update is **In a Call**, the Polycom CMA system waits until the call ends before updating the endpoint. The system checks the endpoint at 15 minute intervals.
- If an endpoint scheduled for update is **Offline**, the Polycom CMA system attempts to connect to the endpoint every hour until the endpoint is **Online**.
- A software update may reboot the endpoint.

Endpoint Passwords

A Polycom CMA system can manage Polycom endpoints only when the password in the device record matches the password in the endpoint. Matching passwords are required to:

- Schedule provisioning of an endpoint through a Polycom CMA system
- Use the Scheduled Softupdate feature
- Monitor the endpoint from the **Endpoint > Monitor View**

You can update the password for certain endpoint systems through scheduled provisioning only after you have entered the matching password in the Polycom CMA system. In this case, you must instruct end-users not to change the password.

Note

Some companies select an administrative password that is used for all endpoints and regularly updated through provisioning.

For third-party endpoints, passwords may be required to access the endpoint management software.

For information about restrictions in changing passwords for a specific endpoint, see the documentation for the endpoint.

8

Endpoint Management Operations

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA™) system endpoint management tasks. It includes these topics:

View Device Details

To view detailed information about a managed endpoint

1. Go to **Endpoint > Monitor View**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoint of interest and click **View Details**.

   The **Device Details** dialog box for the selected endpoint appears.

Field	Description
Identification	
System Name	The name of the endpoint. • Endpoint names must be unique. • The name must be in ASCII only[a] and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. • When retrieved from a video endpoint system, the name is taken from the H.323 ID if the endpoint registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.
Device Type	The type of endpoint. For valid types, see "Endpoint Types" on page 61.
IP Address	The assigned IP address of the endpoint
Owner	The user to whom the endpoint is assigned
Description	A free-form text field (Extended ASCII only[a]) in which information about the endpoint can be added
Site	The network site for the endpoint. By default, endpoints are added to the **Primary Site**.
Product ID	
Serial Number	The serial number (ASCII only[a]) of the endpoint.The endpoint provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the endpoint (ASCII only[a]). The endpoint provides the version number if it registered successfully or is managed.
HTTP URL	The management URL for the endpoint, if available (ASCII only[a]). This URL allows the Polycom CMA system to start the endpoint 's management system using the **Manage** function. All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the Polycom CMA system. For third-party endpoints that do not register using an IP address, you must enter the URL.
HTTP Port	The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.

Field	Description
Addresses	
Aliases	The aliases that allow you to connect to the endpoint. The Polycom CMA system converts the aliases to the IP address associated with the endpoint. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown. • The value for the H.323 ID is the endpoint name if the endpoint registered with the gatekeeper and it is a third-party system. In other cases, the endpoint name is the system name, which might be different from the H323 ID. • The value of the E.164 alias is the extension dialed to reach this endpoint. **Note** The following **Alias Values** are ASCII only[a]: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.
ISDN Video Number	For ISDN endpoints only, the country code + city/area code + phone number for the endpoint. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The Polycom CMA system only supports native ISDN.
LAN Host Name	The host name of the endpoint on the LAN. This can be different from the system name of the endpoint. It is an ASCII only[a] name.
Call Signaling Address	
RAS Address	
Capabilities	
Supported Protocols	The communications protocols that the endpoint can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. For endpoints with the type **Unknown**, select **H.323**. The endpoint automatically provides the protocols if it registered successfully or is managed.

Field	Description
Capabilities Enabled	Capabilities to enable on this endpoint. Options are: • **MCU** - The device can act as a control unit for multipoint conferences • **Gateway** - The device can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed.
Available to Schedule	Select this option to make the endpoint available when users are scheduling conferences
Monitoring Level	The monitoring level for the endpoint. Possible values include: • **Standard.** This endpoint is monitored. • **VIP.** This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Admin ID	The ID for the endpoint administrator
Call Info > Sites	
Connection Status	State of the endpoint. Possible values include: **In a Call**, **Online**, or **Offline**
Call type	The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and SIP
Far Site Info	**Site**— **Name**—The H.323ID of the far site device to which the selected endpoint is connected. When multiple endpoints are connected through the device's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' | ', e.g. 'ISDN-CO1-7-1 | Vsfx-9-1'. **Number**—The address of the far site device to which the selected endpoint is connected. The address value for the calling device appears to be the dialed address. The address value for the called device appears to be the IP Address. **Encryption**—The type of encryption the far site uses
Call Info > Call Details	

Field	Description
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the device is using
Video Rate	The video bandwidth negotiated with the far site
Video Rate Used	The actual video bandwidth used in the call to the far site
Video Frame Rate	
Video FEC Errors	
Cause Code	The cause code showing how the call ended.
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • G.711 • G.722 • G.728
Audio Rate	The audio bandwidth negotiated with the far site
Call Info > Quality of Service	
Total Packet Loss	
% Packet Loss	
Audio Packet Loss	
Video Packet Loss	
Audio Jitter	
Video Jitter	
Call Info > Far Site Details	
Tx Call Speed	The call s
Rx Call Speed	
Error	

Field	Description
Sync	
Call Type	
System Alerts	
Errors	Device error message text, e.g., GK Registration error
Warnings	Device warning message text, e.g., Low Battery

a. For more information on field limitations, see “Field Input Requirements” on page 6.

Add an Endpoint or Find an Endpoint on the Network

This section describes how to manually add endpoints and how to find endpoints on the same network as the Polycom CMA system.

For most endpoints, you enter basic information. The Polycom CMA system then locates the endpoint and retrieves its device details.

To add an endpoint to a Polycom CMA system or find an endpoint on the network

1. Go to **Endpoint > Monitor View** and click **Add**  .
2. In the **Add New Device** dialog box, select the **Device Type** of interest. For valid types, see "Endpoint Types" on page 61. For third-party endpoints, select a **Device Type** of **Other**.
3. Enter the **IP Address** of the endpoint.
4. If necessary, enter the **Admin ID** and **Password** for the endpoint. Some endpoints may not require this information. Other endpoints may require only a password.
5. Click **Find Device**.
   - If the Polycom CMA system can find the endpoint on the network, the **Add New Device** dialog box is populated with information retrieved from the endpoint. Review any information retrieved from the endpoint.
   - If the Polycom CMA system cannot find the endpoint on the network, a **Device Not Found** dialog box appears.

Note

If you enter an invalid **Admin ID** or **Password** for an endpoint that requires that information, the Polycom CMA system may still find the endpoint. It depends upon the endpoint type.

- V-Series, VSX-Series, and Viewstation endpoints allow the Polycom CMA system to detect the endpoint type and complete the registration. The endpoint appears in the **Endpoint** list with an alert indicating **Incorrect Password**.
- Polycom HDX systems and ViewStation FX systems won't allow the Polycom CMA system to detect the endpoint type and complete the registration. You can manually add the endpoint, but the Polycom CMA system cannot communicate with it until you've entered a valid **Admin ID** or **Password** for the endpoint. In this case, the Polycom CMA system records an error message in a device error log.

6. Click **OK**.

7 Complete the **Identification**, **Addresses,** and **Capabilities** sections of the **Add New Device** dialog box. (For more information, see "View Device Details" on page 95.) At a minimum, assign the endpoint a **System Name**.

Pay particular attention to the **Capabilities** options, because the settings on it determine how the endpoint is used throughout the Polycom CMA system. For example, you can select it as a **VIP** endpoint and determine whether it will be **Available to Schedule** through the scheduling interface.

Note that many fields in this dialog box are ASCII only. For more information, see "Field Input Requirements" on page 6.

8 Click **Add**.

The endpoint appears in the **Endpoint** list. By default, the system:

- Adds the endpoint to the applicable site
- Sets the **HTTP Port** to 80
- Adds an **Alias** for the endpoint
- Makes the endpoint **Available to Schedule**
- Sets the **Monitoring Level** to **Standard**

Note

For third-party endpoints, the HTTP URL, serial number, and DNS name are not captured during endpoint registration.

Once you've added an endpoint, you can associate it with a user. See "Assign Users Roles and Devices" on page 184.

Edit an Endpoint

The Polycom CMA system automatically detects IP address changes and updates its database with the new information for Polycom and third-party endpoints that are registered with the Polycom CMA system.

To edit an endpoint in the Polycom CMA system

1 Go to **Endpoint > Monitor View**

2 As needed, use the **Filter** to customize the endpoint list.

3 Select the endpoint of interest and click **Edit**  .

4 As required, edit the **Identification**, **Addresses,** and **Capabilities** sections of the **Edit Device** dialog box. (For more information, see "View Device Details" on page 95.)

Note that many fields in this dialog box are ASCII only. For more information, see "Field Input Requirements" on page 6.

5 Click **Update**.

Note

Editing information for endpoint management by the Polycom CMA system does not change the information in the endpoint. To make changes in the endpoint information, use **Provisioning** or change it at the endpoint interface. Note that for managed endpoints, the endpoint may overwrite settings entered manually.

Delete an Endpoint

To delete an endpoint from the Polycom CMA system

1 Go to **Endpoint > Monitor View**

2 As needed, use the **Filter** to customize the endpoint list.

3 Select the endpoint of interest and click **Delete** .

4 Click **Yes** to confirm the deletion.

The **Endpoint** list is updated.

Note

If your gatekeeper registration policy allows endpoints to register automatically with the Polycom CMA system (i.e., a gatekeeper setting of **Allow Registration of All Endpoints** or **Allow Registration of Endpoints in Defined Sites** or **Allow Registration of Predefined Prefixes Only**) a endpoint that you delete may reappear in the **Endpoint** list.

View an Endpoint's Video Feed

Note

This procedure is available on the following endpoint types:

- Polycom HDX system
- Tandberg
- V-Series and VSX-Series
- ViewStation

To view the video feed for an endpoint (near site or far site)

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest and click **View Details**.

   The **Device Details** dialog box appears. For information about these fields, see "View Device Details" on page 95.
4. Click **Call Info** to expand the **Call Info** options and select **Video Feed**.

   The **Endpoint Video** section shows the video feed from the near and far site.

Clear an Endpoint Help Request

To clear an endpoint help request from the Polycom CMA system

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest and click **Clear Help**.

   The **Confirm Endpoint Help Clear** dialog box appears.
4. To send a message to the endpoint as well as clear the help request, check **Also send message to endpoint**.
5. Click **Clear**.
6. If you selected the **Also send message to endpoint** checkbox, enter the text message to send the endpoint in the **Send Message to Endpoint** dialog box and click **Send**. (Note that the text-message field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

   The **Endpoint** list is updated and alerts for the endpoint are cleared.

> **Note**
> If the reason for the original alert still exists on the endpoint, the alert will likely reappear in the **Endpoint** list.

Send a Message to an Endpoint

In some situations, such as in response to a help request, you can send a message to some types of endpoints.

To send a message to an endpoint from the Polycom CMA system

1 Go to **Endpoint > Monitor View**

2 As needed, use the **Filter** to customize the **Endpoint** list.

3 Select the endpoint of interest.

If the endpoint can receive text messages, a **Send Message** option appears in the **Command** menu.

4 Click **Send Message**.

5 In the **Send Message to Endpoint** dialog box, enter a text message and click **Send**. (Note that the text-message field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

The message is sent to the endpoint.

9

Endpoint Provisioning Operations

This chapter discusses Polycom® Converged Management Application™ (CMA™) system automatic and scheduled endpoint provisioning operations.

For automatic endpoint provisioning, it includes these topics:

- View the Automatic Provisioning List and Details
- Add an Automatic Provisioning Profile
- Edit an Automatic Provisioning Profile
- Edit the Profile Order for an Automatic Provisioning Profile
- Clone an Automatic Provisioning Profile
- Delete an Automatic Provisioning Profile

For scheduled endpoint provisioning, it includes these topics:

- View the Scheduled Provisioning List and Details
- Add a Scheduled Provisioning Profile
- Edit a Scheduled Provisioning Profile
- Clone a Scheduled Provisioning Profile
- Delete a Scheduled Provisioning Profile
- Schedule an Endpoint for Provisioning
- Check the Status of a Scheduled Provisioning
- Clear the Status of Scheduled Provisioning
- Cancel a Scheduled Provisioning

Automatic Provisioning Operations

View the Automatic Provisioning List and Details

To view the automatic provisioning list and details about an automatic provisioning operation

1. Go to **Endpoint > Automatic Provisioning**.
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Expand the **Provisioning Details** tab in the **Device Details** section.

Add an Automatic Provisioning Profile

This section describes how to add automatic provisioning profiles.

TIP
Add provisioning profiles in the middle of the work day, not first thing in the morning.

When you add an automatic provisioning profile, the Polycom CMA system immediately rolls it out. If it rolls it out first thing in the morning, people who need to attend a "start the day" meeting will have to first wait for their endpoint to be provisioned. Better to implement profiles in the middle of the work day and then let the provisioning occur at the designated polling interval.

To add an automatic provisioning profile

1. Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
2. In the **Automatic Provisioning Profiles** page, click **Add**  .
3. In the **Add Profile** dialog box, enter a name for the profile and click **Next**.
4. Complete the **System Settings, Home Screen Settings**, **H.323 Settings**, **Call Settings**, **Audio Settings**, and (if applicable) **CMA Desktop Settings** sections of the **Provisioning Fields** dialog box.

   For information about these fields, see "Automatic Device Provisioning" on page 72. The sections may differ depending on the endpoint type selected.

5 Click **OK**.

The provisioning profile appears at the bottom **Automatic Provisioning Profiles** list.

6 To change the priority order of the automatic provisioning profiles:

a Click in the **Profile Order** text box preceding the provisioning profile of interest and enter the priority for the profile.

b Click **Update Profile Order**.

The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

Edit an Automatic Provisioning Profile

To edit an automatic provisioning profile

1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.

2 In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Edit**  .

3 Edit the **System Settings, Home Screen Settings**, **H.323 Settings**, **Call Settings**, **Audio Settings**, and (if applicable) **CMA Desktop Settings** sections of the **Provisioning Fields** dialog box.

For information about these fields, see "Automatic Device Provisioning" on page 72. The sections may differ depending on the endpoint type selected.

4 Click **OK**.

The provisioning profile is updated.

Edit the Profile Order for an Automatic Provisioning Profile

To edit the profile order for an automatic provisioning profile

1 Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.

2 In the **Automatic Provisioning Profiles** page, select the profile of interest, click in the **Profile Order** text box preceding the provisioning profile of interest, and enter the priority for the profile.

3 Click **Update Profile Order**.

The system assigns the provisioning profile the selected priority and shuffles and reassigns priorities to the other provisioning profiles.

Clone an Automatic Provisioning Profile

To clone an automatic provisioning profile

1. Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
2. In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Clone**  .
3. In the **Clone Profile** dialog box, enter a name for the new profile and click **Save**.

   The provisioning profile appears last in the **Automatic Provisioning Profiles** list.
4. As needed, edit the profile. See "Edit an Automatic Provisioning Profile" on page 109.

Delete an Automatic Provisioning Profile

To delete an automatic provisioning profile

1. Go to **Admin > Provisioning Profiles > Automatic Provisioning Profiles**.
2. In the **Automatic Provisioning Profiles** page, select the profile of interest and click **Delete**  .
3. Click **Yes** to confirm the deletion.

   The profile is deleted from the Polycom CMA system.

Scheduled Provisioning Operations

View the Scheduled Provisioning List and Details

To view the automatic provisioning list and details about a scheduled provisioning operation

1. Go to **Endpoint > Scheduled Provisioning**.
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Expand the **Provisioning Details** tab in the **Device Details** section.

Add a Scheduled Provisioning Profile

To add a scheduled provisioning profile

1. Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
2. In the **Scheduled Provisioning Profiles** page, click **Add**  .
3. In the **Add Profile** dialog box, select the **Endpoint Type** for the provisioning profile, enter a name for the profile, and click **Next**.
4. As needed, select **Provision This Page** and complete the **General Settings, Video Network**, **Monitors**, **Cameras**, **Audio Settings**, **LAN Properties**, and **Global Services** sections of the **Provisioning Fields** dialog box.

   For information about these fields, see "Automatic Device Provisioning" on page 72. The sections may differ depending on the endpoint type selected.
5. Click **OK**.

   The provisioning profile appears in the updated **Scheduled Provisioning Profiles** list.

Edit a Scheduled Provisioning Profile

To edit a scheduled provisioning profile

1. Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
2. In the **Scheduled Provisioning Profiles** list, select the profile of interest and click **Edit Profile**.
3. Edit the sections of the **Provisioning Fields** dialog box. The sections and fields differ depending on the endpoint type selected. For more information on these fields, see the product documentation for the selected endpoint.
4. Review each page of the scheduled provisioning profile and determine if you want the parameters on the page provisioned. If you do want the parameters on the page provisioned, select **Provision This Page**.
5. Click **OK**.

   The provisioning profile is updated.

Clone a Scheduled Provisioning Profile

To clone a scheduled provisioning profile

1. Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
2. In the **Scheduled Provisioning Profiles** page, select the profile of interest and click **Clone Profile**.
3. In the **Clone Profile** dialog box, enter a name for the new profile and click **Save**.

   The provisioning profile appears first in the updated **Scheduled Provisioning Profiles** list.

   As needed, edit the cloned profile. See "Edit a Scheduled Provisioning Profile" on page 111.

Delete a Scheduled Provisioning Profile

To delete a scheduled provisioning profile

1. Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
2. In the the **Scheduled Provisioning Profiles** page, select the profile of interest and click **Delete Profile**.
3. Click **Yes** to confirm the deletion.

   The profile is deleted from the Polycom CMA system.

Schedule an Endpoint for Provisioning

To schedule an endpoint for provisioning

1. Go to **Endpoint > Scheduled Provisioning** .
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoints of interest.
4. Click **Provision**.
5. In the **Schedule Endpoint Provisioning** dialog box, select the appropriate provisioning profile.
6. In the **Schedule** field, select **Now** or **Later**.
7. If you select **Later**, enter a **Date** and **Time** for the provisioning.

8 Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.

9 Click **Schedule**.

The **Scheduled Provisioning View** reappears.

10 Click **Refresh** and check the **Pending** column for the provisioning status.

For each endpoint you selected, the name of the profile appears in the **Pending** column, and the date and time you entered appears in the **Scheduled** column.

Check the Status of a Scheduled Provisioning

To check the status of a scheduled provisioning

1 Go to **Endpoint > Scheduled Provisioning**.

2 As needed, use the **Filter** to customize the endpoint list.

3 Select the endpoint of interest.

4 Expand the **Provisioning Details** tab in the **Device Details** section.

For information about the fields in this section, see "View the Scheduled Provisioning List and Details" on page 110.

Clear the Status of Scheduled Provisioning

To clear the status of a scheduled provisioning

1 Go to **Endpoint > Scheduled Provisioning**.

2 As needed, use the **Filter** to customize the endpoint list.

3 Select the endpoints of interest.

4 Click **Clear Status**.

The endpoint provisioning status returns to **Clear**.

Cancel a Scheduled Provisioning

You can only cancel provisioning of a **Pending** process. You cannot cancel the provisioning of an endpoint while it is **In Progress**.

To cancel a pending scheduled provisioning

1. Go to **Endpoint > Scheduled Provisioning**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoints of interest.
4. Click **Cancel Provision**.

   The provisioning operation is cancelled and the provisioning status returns to **Clear**.

10

Endpoint Softupdate Operations

This chapter describes how to use Polycom® Converged Management Application™ (CMA™) system to update the software on Polycom endpoints when a new software package is available.

For automatic softupdate, it includes these topics:

- View Automatic Softupdate Information
- View Automatic Softupdate Packages
- Implement Automatic Softupdates for Endpoints

For scheduled softupdate, it includes these topics:

- View Scheduled Softupdate Information
- View List of Softupdate Packages
- Implement Scheduled Softupdates for Endpoints

Automatic Softupdate Operations

View Automatic Softupdate Information

To view information for endpoints that are eligible for automatic softupdates

1. Go to **Endpoint > Automatic Softupdate** .

   The **Automatic Softupdate** page appears.
2. As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.
3. Select the endpoint of interest.
4. In the **Device Details** section, expand the **Softupdate Details** tab. For more information, see "Softupdate Details" on page 137.

View Automatic Softupdate Packages

To view the list of automatic softupdate packages

1 Go to **Admin > Software Updates > Automatic Software Updates**.

The **Automatic Software Updates** page appears and the Polycom HDX Series automatic softupdate packages are displayed. The **Automatic Software Updates** page includes this information.

Field	Description
Version to use	Displays the default automatic softupdate profile to be used for the endpoint type and model
Allow this version or newer	When checked, indicates that when a newer automatic softupdate package for the endpoint type and model is added, that package should be used as the default package
Endpoint Type	The type of endpoint system. For valid endpoint system types, see "Endpoint Configuration/Provisioning" on page 71.
Version	The version of the software package associated with the automatic softupdate package
Description	The meaningful name given to the automatic softupdate package when it was created
Uploaded	The date and time when the automatic softupdate package was created
Trial Group	The trial group assigned to the software update package, if applicable.

2 To view the Polycom CMA Desktop automatic softupdate packages, click the **CMA Desktop** tab.

Implement Automatic Softupdates for Endpoints

To implement automatic softupdates, complete the following tasks:

1 "List the Serial Numbers for the Endpoints to be Updated" on page 117.

2 "Download the Required Software Package" on page 118.

3 "Request Update Activation Keys" on page 118.

4 "Upload the Software Package and Create a Softupdate Package" on page 119. For more information on softupdate packages, see "View Automatic Softupdate Information" on page 115.

5 "Set an Automatic Softupdate Policy" on page 120.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

1 Go to **Admin > Software Updates > Automatic Software Updates**.

2 Click **Get Serial Numbers**  .

The **Endpoint Serial Number List** appears listing the endpoints eligible for automatic softupdate. Devices without serial numbers and devices that are not actively managed by the system are excluded.

The **Automatic Software Updates** page includes this information.

Field	Description
Type	
Model	
Name	The name assigned to the endpoint system
IP Address	
Version	
Site	

3 As needed, use the **Filter** to customize the endpoint list.

4 Select the specific endpoints to be updated. To select all devices in the list, click the checkbox in the column header.

5 Click **Get Serial Numbers**.

The serial number(s) appear in the text box on the page.

6 When updating a single endpoint:

a Record the serial number:_____

b Click **Close**.

The **Automatic Software Updates** list reappears.

c Go to "Download the Required Software Package" on page 118.

7 When updating multiple endpoints:

a Copy and paste the serial numbers from the list to a `.txt` file that you can submit to the **Polycom Product Activation** site. Put one serial number per line as shown in the following example.

```
82071007E1DACD
82070407E010CD
820418048078B2
82040903E00FB0
```

b Return to the **Endpoint Serial Number List** and click **Close**.

The **Automatic Software Updates** list reappears.

c Repeat steps 2 through 7 for the each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same `.txt` file.

d Save the `.txt` file.

e Go to "Download the Required Software Package" on page 118.

Download the Required Software Package

To download the software package required to update the devices

1 On your local system, create a directory to which to save the software package (if one does not already exist).

2 With a web browser, go to `www.polycom.com/support`.

3 In the **Downloads** section, select the **Product** and **Category** for the required software package.

4 Select the software package and save it to the directory created in step 1.

5 Repeat steps 3 through 4 for each device type to be updated. Note that the software package may contain the software for different models of the same device type.

Request Update Activation Keys

Note

In general, you need an activation key when updating to a major release (for example, 3.x to 4.x) or minor release (for example, 3.1 to 3.2). You do not need an activation key when updating a point release (for example, 3.1.1 to 3.1.2). However, you should read the product release notes for specific information about whether or not you'll need an activation key.

To request upgrade activation keys

1 Go to **http://www.polycom.com/activation**.

2 Log in or **Register for An Account**.

3 Select **Product Activation**.

4 In the **Software Upgrade KeyCode** section, click **Retrieve Software KeyCode**.

5 When upgrading a single device:

   a Enter the serial number of the device to be updated into the **Serial Number** field of the **Single Upgrade Key Code** section.

   b Enter the version number to which you are upgrading and click **Retrieve**.

      The key code is returned on the screen.

   c Record the key code and create a `.txt` file with the Serial Number - Key Code combination to be updated.

   d Close the **Product Activation** screens.

6 When updating multiple devices from a prepared `.txt` file (step 7 on page 117):

   a In the **Multiple Upgrade KeyCode** section, click **Add Attachment**.

   b Browse to the location of the `.txt` file you created in step 7 on page 117 and click **Upload**.

      A file containing the Serial Number - Key Code combinations will be emailed to the specified email account.

   c When you receive the `.txt` file, save it to your local system.

   d Close the **Product Activation** screens.

Upload the Software Package and Create a Softupdate Package

After you receive notification about a new software package for a Polycom endpoint, upload the softupdate to the Polycom CMA system and create a softupdate profile to use for the update.

To upload the software package and create an automatic softupdate profile

1 Go to **Admin > Software Updates > Automatic Software Updates**.

2 Select the tab for the endpoint type of interest.

3 Click **Upload Software Update**.

4 In the **Upload Software Update** dialog box, verify the endpoint type and model.

5 If an activation key code is required to activate the softupdate, click the **Update Requires Key** checkbox and in the **Software Update Key File** field browse to the `.txt` key file received in "Request Update Activation Keys" on page 118 .

Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at `http://www.polycom.com/support`.

6 Enter a meaningful description that will help other users to understand the purpose of the softupdate. (Note that the field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

7 Click **OK**.

An automatic softupdate profile for the endpoint type and model type appears in the **Automatic Software Updates** list.

If you receive a message that indicates "This version is the first for its endpoint type, so it will be assumed to be the policy for this endpoint type," the softupdate profile also appears in the **Version to use** field.

Set an Automatic Softupdate Policy

To set an automatic softupdate policy for an endpoint type

1 Go to **Admin > Software Updates > Automatic Software Updates**.

2 Select the tab for the endpoint type of interest.

3 Choose one of these policies:

- To specify a minimum version of automatic softupdate package, make that version the **Version to use** and select **Allow this version or newer**.
- To require a specific version of automatic softupdate package, make that version the **Version to use** and clear **Allow this version or newer**.
- To turn automatic softupdate off for an endpoint type, change the **Version to use** value to **(none)**.

4 Click **Update**.

Trial a Softupdate Package

To trial a softupdate package:

1. Get the things you need to create the package. Complete these tasks:
   a. "List the Serial Numbers for the Endpoints to be Updated" on page 117.
   b. "Download the Required Software Package" on page 118.
   c. "Request Update Activation Keys" on page 118.
2. Set up testing. Complete these tasks:
   a. "Create a Local Trial Group" on page 121.
   b. "Upload the Software Package and Create a Trial Softupdate Package" on page 121. For more information on softupdate packages, see "View Automatic Softupdate Information" on page 115.
3. Once your testing of the trial software package is complete, do one of these tasks:
   - "Promote the Trial Softupdate Package to Production" on page 122
   - "Delete the Trial Softupdate Package" on page 123.

Create a Local Trial Group

To trial a software update with a specific group of local and/or enterprise users, create a local group that includes these users, as described in "Add a Local Group" on page 181. The people in this group will receive the trial softupdate package when their endpoint goes through its normal, automated softupdate process.

Notes

- You can use an existing enterprise group as a trial group, but you will not be allowed to change the enterprise group in any way.
- If the trial software group is a parent group with children, all of its children will inherit trial permissions.

Upload the Software Package and Create a Trial Softupdate Package

To upload the software package and create a trial automatic softupdate package

1. Go to **Admin > Software Updates > Automatic Software Updates**.
2. Select the tab for the endpoint type of interest.

3 Click **Upload Software Update**.

4 In the **Upload Software Update** dialog box, verify the endpoint type and model.

5 If an activation key code is required to activate the softupdate, click the **Update Requires Key** checkbox and in the **Software Update Key File** field browse to the `.txt` key file received in "Request Update Activation Keys" on page 118 .

Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at `http://www.polycom.com/support`.

6 Enter a meaningful description that will help other users to understand the purpose of the softupdate. (Note that the field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

7 To trial the software with the group created previously, select **Trial Software** and from the **Select Trial Group** menu, select the trial group created in "Create a Local Trial Group" on page 121.

8 Click **OK**.

A trial automatic softupdate package for the endpoint type and model type appears in the **Automatic Software Update** list. You can tell it is a trial package, because the **Trial Group** column includes your entry.

The next time members of the trial group log into the system, their systems will be upgraded with the trial software package.

Promote the Trial Softupdate Package to Production

If you determine that the trial softupdate package is acceptable for production, you can then promote it to production.

To promote a trial softupdate package to production

1 Go to **Admin > Software Updates > Automatic Software Updates**.

2 Select the tab for product to update.

3 Select the softupdate package of interest and click **Promote to Production**.

4 Click **Yes** to confirm the promotion.

The package becomes a production automatic softupdate package.

Delete the Trial Softupdate Package

If you determine that the trial softupdate package is unacceptable for production, you can delete it.

To delete a trial softupdate package

1. Go to **Admin > Software Updates > Automatic Software Updates**.
2. Select the tab for product to update.
3. Select the softupdate package of interest and click **Delete Software Update**.
4. Click **Yes** to confirm the deletion.

   The package is removed from the **Automatic Software Updates** list.
5. To return your trial group to the last production version of software, clear the **Allow this version or newer** option and click **Update**.
6. When all endpoints are back to the last production version of software, reset your automatic softupdate policy. See "Set an Automatic Softupdate Policy" on page 120.

Scheduled Softupdate Operations

View Scheduled Softupdate Information

To view information about softupdates that are schedule or for endpoints that are eligible for scheduled softupdates

1. Go to **Endpoint > Scheduled Softupdate**.
2. As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.
3. Select the endpoint of interest.
4. In the **Device Details** section, expand the **Softupdate Details** tab. For more information, see "Softupdate Details" on page 137.

View List of Softupdate Packages

To view the list of scheduled softupdate packages

>> Go to **Admin > Software Updates > Scheduled Software Updates**.

The **Scheduled Software Updates** page appears and includes this information.

Field	Description
Endpoint Type	The type of endpoint. For valid types, see "Endpoint Types" on page 61.
Endpoint Model	The model of endpoint
Description	The meaningful name given to the automatic softupdate package when it was created
Uploaded	The date and time when the scheduled softupdate package was created

Implement Scheduled Softupdates for Endpoints

To implement the automatic softupdate process you must perform this series of tasks.

1. "List the Serial Numbers for the Endpoints to be Updated" on page 124.
2. "Download the Required Software Package" on page 126.
3. "Request Update Activation Keys" on page 118.
4. "Upload the Software Package and Create a Softupdate Package" on page 119. For more information on softupdate profiles, see "View Automatic Softupdate Information" on page 115.
5. "Schedule the Softupdate for Endpoints" on page 127.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

1. Go to **Admin > Software Updates > Scheduled Software Updates**.
2. Select the appropriate **Endpoint Type** and **Endpoint Model** combination for the endpoint to update.

3 Click **Get Serial Numbers** .

The **Endpoint Serial Number List** appears listing the devices of the selected type and model that are eligible for scheduled softupdates. The page includes this information.

Field	Description
Type	
Model	
Name	The name assigned to the endpoint system
IP Address	
Version	
Site	

4 As needed, use the **Filter** to customize the endpoint list.

5 Select the specific endpoints to be updated. To select all devices in the list, click the checkbox in the column header.

6 Click **Get Serial Numbers**.

The serial number(s) appear in the text box on the page.

7 When updating a single device:

a Record the serial number:_____

b Click **Close**.

The **Scheduled Software Updates** list reappears.

8 When updating multiple devices:

a Copy and paste the serial numbers from the **Endpoint Serial Number List** to a `.txt` file that you can submit to the **Polycom Product Activation** site. Put one serial number per line as shown in the following example.

```
82071007E1DACD
82070407E010CD
820418048078B2
82040903E00FB0
```

b Return to the **Endpoint Serial Number List** and click **Close**.

The **Scheduled Software Updates** list reappears.

c Repeat steps 2 through 8 for the each device or set of devices to be updated. You may include all of the serial numbers for all of the different device types in the same `.txt` file.

d Save the `.txt` file.

Download the Required Software Package

To download the software package required to update the devices

1. On your local system, create a directory to which to save the software package (if one does not already exist).
2. With a web browser, go to `www.polycom.com/support`.
3. In the **Downloads** section, select the **Product** and **Category** for the required software package.
4. Select the software package and save it to the directory created in step 1.
5. Repeat steps 3 through 4 for each device type to be updated. Note that the software package may contain the software for different models of the same device type.

Request Update Activation Keys

To request upgrade activation keys

1. Go to **http://www.polycom.com/activation**.
2. Log in or **Register for An Account**.
3. Select **Product Activation**.
4. In the **Software Upgrade KeyCode** section, click **Retrieve Software KeyCode**.
5. When upgrading a single device:
   a. Enter the serial number of the device to be updated into the **Serial Number** field of the **Single Upgrade Key Code** section.
   b. Enter the version number to which you are upgrading and click **Retrieve**.

      The key code is returned on the screen.
   c. Record the key code and create a `.txt` file with the Serial Number - Key Code combination to be updated.
   d. Close the **Product Activation** screens.
6. When updating multiple devices from a prepared `.txt` file (step 7 on page 117):
   a. In the **Multiple Upgrade KeyCode** section, click **Add Attachment**.
   b. Browse to the location of the `.txt` file you created in step 7 on page 117 and click **Upload**.

      A file containing the Serial Number - Key Code combinations will be emailed to the specified email account.

c When you receive the `.txt` file, save it to your local system.

d Close the **Product Activation** screens.

Upload the Software Package and Create a Softupdate Profile

To upload the software package and create an automatic softupdate profile

1 Go to**Admin > Software Updates > Scheduled Software Updates**.

2 On the **Software Update Profiles** list, click the checkbox to select the appropriate **Endpoint Type** and **Endpoint Model** combination for the endpoints to be updated. To select all endpoints in the list, click the checkbox in the column header..

3 In the **Upload Software Update** dialog box, verify the endpoint type and model.

4 If an activation key code is required to activate the softupdate, click **Update Requires Key** and in the **Software Update Key File** field browse to the `.txt` key file (received in "Request Update Activation Keys" on page 118) .

Note

The key is generated from the endpoint serial number and version number, and Polycom sends it as a text (`.txt`) file to the customer when new software is available. Customers can review their key history at `http://www.polycom.com/support`.

5 Enter a meaningful description that will help other users to understand the purpose of the softupdate. (Note that the field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

6 Click **OK**.

A scheduled softupdate profile for the endpoint type and model type is created.

7 In a redundant configuration, repeat steps 1 through 6 on the redundant server.

Schedule the Softupdate for Endpoints

To schedule one or more endpoints for softupdate

1 Go to **Endpoint > Scheduled Softupdate**.

2 As needed, use the **Filter** to customize the endpoint list.

3 Select the endpoints of interest and click **Software Update**.

4 In the **Schedule Software Update** dialog box, specify when the update should occur.

   a In the **Schedule** field, select **Now** or **Later**.

   b If you select **Later**, enter a **Date** and **Time** for the update.

   c Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.

5 Select from these options.

Fields	Description
Remove address book entries	Select this checkbox to have all local address book entries removed after the update.
Remove system files	Select this checkbox to have all endpoint settings removed after the update. You must then reconfigure the endpoint.
Allow endpoint to be a DHCP server	Select this checkbox to allow the endpoint to be a DHCP server. Applies to V-Series, VSX-Series, and ViewStation endpoints only. For more information, see the endpoint's user guide.
Passive mode	Select this checkbox to perform a softupdate in passive FTP mode. Applies to V-Series, VSX-Series, and ViewStation endpoints only. For more information, see the endpoint's user guide.

Note

You may apply a single softupdate request to multiple endpoint models. If the request includes one or more scheduling options that are not valid for a selected endpoint model, the system applies only the options that are valid.

6 Click **Schedule**.

For each endpoint selected, the status changes to **Pending** and the date and time for the softupdate appears in the **Scheduled** column.

Cancel Software Updates

You can cancel **Pending** scheduled softupdates for an endpoint. You cannot explicitly cancel automatic softupdates for an endpoint. You must do that at the endpoint.

To cancel pending scheduled software updates

1. Go to **Endpoint > Scheduled Softupdate**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoint of interest and click **Cancel Update**.

   The software update operation is canceled. The endpoint's status returns to **Clear**.

11

Device Details

This chapter lists the fields found in the Device Detail section of the Polycom® Converged Management Application™ (CMA™) system interface. It includes these topics:

Device Summary Information

The **Device Summary** information in the **Device Details** section includes the following fields.

Field	Description
Name	The name of the device
Type	The type of device. For valid device types, see "Endpoint Configuration/Provisioning" on page 71.
Owner	(Endpoints only) The user associated with the device
IP Address	The assigned IP address of the device
ISDN Video Number	For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The CMA system only supports native ISDN.
Site	The network site for the device. By default, devices are added to the **Primary Site**.

Field	Description
Software Version	The version of the software installed on the device (ASCII only[a]). The device provides the version number if it registered successfully or is managed.
Serial Number	The serial number (ASCII only[a]) of the device.The device provides the serial number if it registered successfully or is managed.
Available to Schedule	Select this option to make the device available when users are scheduling conferences **Note** The **Available to schedule** field is empty and disabled for MGC and RMX 2000 devices.
Monitoring Level	The monitoring level for the device. Possible values include: • **Standard.** This device is monitored. • **VIP.** This device is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Supported Protocols	The communications protocols that the device can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. For devices with the type **Unknown**, select **H.323**. The device automatically provides the protocols if it registered successfully or is managed. **Notes** • If an endpoint is configured as a gateway (ISDN), only the **H.323** checkbox is selected. If the endpoint supports true ISDN, the **H.323** and **ISDN** checkboxes are selected. • RMX 2000 devices support only the **H.323** protocol.
Capabilities Enabled	Capabilities to enable on this device. Options are: • **MCU** - The device can act as a control unit for multipoint conferences • **Gateway** - The device can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed. **Note** Currently, RMX 2000 devices cannot be Gateway devices.

Field	Description
Alias (type)	The alias to connect to the device. The CMA system converts the aliases to the IP address associated with the device. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown.

a. For more information on field limitations, see "Field Input Requirements" on page 6.

Device Status Information

The **Device Status** information in the **Device Details** section includes the following fields.

Field	Description
Gatekeeper Registration	The status of the device's registration with the gatekeeper service. Possible values include: • Registered  • Unregistered 
GDS Registration	The status of the device's registration with the Global Directory Service. Possible values include: • Registered  • Unregistered 
Presence Registration	The status of the device's registration with the presence service. Possible values include: • Registered  • Unregistered 
GK Registration Timeout	The gatekeeper registration expiration date and time for the device in a default format of `mm-dd-yyyy hh:mm:ss AM | PM` with adjustment to the client-machine GMT offset.
Last GK Registration	The date and time of the device's last gatekeeper registration in a default format of `mm-dd-yyyy hh:mm:ss AM | PM` with adjustment to the client-machine GMT offset
Device Local Time	The local time as set within the device in a default format of `hh:mm:ss AM | PM`. This field is blank for the following device types: **MGC**, **RMX**, **GW/MCU**, **Other**, and **Tandberg**.

Field	Description
ISDN Line Status Type	The status of the ISDN line. Possible values include: • Operational  • Non-operations  This field is blank for the following device types: **PVX**, **MGC**, **RMX**, **GW/MCU**, **Other**, and **Tandberg**.
ISDN Assignment Type	How the ISDN type was assigned to the device. Possible values include: • **Administrator**, when the ISDN type was assigned manually by an administrator • **Endpoint**, when the ISDN type was natively assigned in the endpoint • **Auto-Assigned**, when the ISDN type was automatically assigned by the CMA system based on the site configuration • **From Network**, when the ISDN type was derived from the gateway and extension • **Undefined**, when the CMA system cannot identify the source for the ISDN type assignment This field is blank for the following device types: **PVX**, **MGC**, **RMX**, **GW/MCU**, **Other**, and **Tandberg**.
Endpoint ISDN Type	The ISDN network interface type installed in the device. Possible values include: • ISDN_QUAD_BRI • ISDN_PRI_T1 • ISDN_BRI • ISDN_UNKNOWN This field is blank for the following device types: **PVX**, **MGC**, **RMX**, **GW/MCU**, **Other**, and **Tandberg**.

Call Information

The **Call Info** in the **Device Details** section includes the following fields.

Field	Description
Call Type	The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and SIP
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the device is using.
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • G.711 • G.722 • G.728
Far Site Name	The H.323ID of the far site device to which the selected endpoint is connected. When multiple endpoints are connected through the device's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' | ', e.g. 'ISDN-CO1-7-1 | Vsfx-9-1'.
Far Site Number	The address of the far site device to which the selected endpoint is connected. The address value for the calling device appears to be the dialed address. The address value for the called device appears to be the IP Address.
Cause Code	Standard H.323 cause code that reflects normal call termination or the nature of an internal failure, e.g., '16' or '211'.
Encryption	The status of encryption for the call. Possible values include: Off, Disabled, AES, and DH-1024

Device Alerts Information

The **Device Alerts** information in the **Device Details** section includes the following fields.

Field	Description
Errors	Device error message text, e.g., GK Registration error
Warnings	Device warning message text, e.g., Low Battery

Provisioning Details

The **Provisioning Details** information in the **Device Details** section includes the following fields.

Field	Description
Last Profile Applied	The name of the last provisioning profile that was or was not successfully applied to the device. The **Provisioning Status** will be either **Success** or **Failed**.
Provisioning Status	The device's current provisioning status. Possible values include: • **Clear.** No provisioning has been done. • **Pending.** Provisioning is scheduled for this device. • **In Progress.** The device is currently being provisioned. • **Success.** Provisioning has been completed successfully on this device. • **Failed.** Provisioning was not completed on this device.
Pending Profile	The name of the provisioning profile that is scheduled to be applied to the device. In this case, the **Provisioning Status** will be either **Pending** or **In Progress**. This field is blank if the device is not scheduled for provisioning.
Scheduled	The date and time, in the default format of `yyyy-mm-dd hh:mm`, when the device is schedule to be provisioned. This field is blank if the device is not scheduled for provisioning.
Last Attempt Date/Time	The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last provisioning message exchanged with the device.

Field	Description
Failure Reason	A text description of the reason the provisioning failed. Causes for failure include: • The provisioning profile does not exist • The provisioning profile does not include provisioning information • The CMA system no longer manages the device • A password for the device is set in the video endpoint system, and you must enter it in the CMA system • The device is busy • A network error occurred • An incomplete transfer of provisioning information occurred • Provisioning has timed out • An internal error occurred on the device, and you must reboot it • An unknown error occurred. Reboot the device.
Log Message	A read-only text box that contains messages related to the device provisioning status

Softupdate Details

The **Softupdate Details** information in the **Device Details** section includes the following fields.

Field	Description
Softupdate Status	The device's software update status. Possible values include: • Clear. A software update has not been done. • Pending. A software update has been scheduled and is pending. The device may be offline or in a call. • In Progress. The software update is in progress. • Success. A software update has completed successfully. • Failed. A software update could not be performed.
Scheduled	The date and time, in the default format of `yyyy-mm-dd hh:mm`, when the device software is schedule to be updated. This field is blank if the device is not scheduled for provisioning.
Last Attempt Date/Time	The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last software update message exchanged with the device.

Field	Description
Failure Reason	A text description of the reason the software update failed. Causes for failure may include: • The software update file location does not exist. • A password for the device is set in the video endpoint system, and you must enter it in CMA. • A network error has occurred. • The update has timed out. • An internal error occurred on the device, and you must reboot it. • A profile has not been configured. • An endpoint is offline. • An incorrect activation key is in the key file. • An unknown error has occurred. Reboot the device
Log Message	A read-only text box that contains the log message text recorded during the execution of the software update. Note that there are no log messages displayed for dynamically-managed endpoints.

12

Network Device Management Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) system's network device management functions. It includes these topics:

Network Device Types

A Polycom CMA system supports these network device types:

- Polycom MGC conferencing bridges
- Polycom RMX conferencing bridges

Notes

- If you have one or more MCUs, you must add a device record for each unit, even when you use the open gatekeeper policy for registration. This process creates a device record for the controller unit.
- Some features such as Lecture Mode, Presentation Mode, Conference on Demand and Chairperson are not available on Polycom RMX 1000 MCUs.

- Polycom Distributed Management Application™ (DMA™) systems
- Polycom Video Border Proxy (VBP) systems

In the **Network Device > Monitor View**, a Polycom CMA system displays MCUs as two separate Device Types, the MCU type and a GW/MCU device.

If automatic registration is allowed, individual H.323 cards and/or IP blades in Polycom MCUs are assigned the device type of **GW/MCU** during registration. This device type represents the cards' network interface. If automatic registration is not allowed, you must add a **GW/MCU** device record for each H.323 card and IP blade.

Network Device Menu, Views, and Lists

The Polycom CMA system **Network Device** menu provides these views of the network device list:

- **Monitor View**—Displays the list of all managable and registered network devices. Use this view to manage network devices.
- **VBPs** (Video Border Proxy systems)—Displays the list of Polycom VBP systems registered to the Polycom CMA system. Use this view to add, edit, or delete VBP systems.
- **MCUs** (Microprocessing Control Units)—Displays the list of Polycom MCUs (Polycom RMX or Polycom MGC conferencing platforms) registered to the Polycom CMA system. Use this view to add, edit, or delete MCUs.
- **DMAs** (Distributed Management Application™ systems)—Displays the list of Polycom DMA™ systems) registered to the Polycom CMA system. Use this view to add, edit, or delete DMA systems.

All of the **Network Device** views have the following information:

Section	Description
Views	The views you can access from the page
Actions	The set of available commands. The constant command in the **Network Device** views is **Refresh** , which updates the display with current information.
Network Device List	The context-sensitive **Network Device** list for the selected view
Device Details	Information about the network device selected in the network device list including: • "Device Summary Information" on page 131 • "Device Status Information" on page 133 • "Call Information" on page 135 • "Device Alerts Information" on page 136 • "Provisioning Details" on page 136 • "Softupdate Details" on page 137

Monitor View

Use the **Network Device > Monitor View** to monitor the network devices.

Network Device List in the Monitor View

By default the **Network Device** list in the **Monitor View** displays a list of network devices the Polycom CMA system monitors, including those devices that registered automatically with the Polycom CMA system and those devices that were added manually for management and monitoring purposes.

The **Network Device** list in the **Monitor View** includes MCUs and Polycom DMA nodes. It does not include Polycom VBP devices.

The **Network Device** list has these fields.

Field	Description
Filter	Use the filter choices to display other views of the **Network Device** list, which include: • **Type**- Filters the list by device type. For more information, see "Network Device Types" on page 139. • **Alerts**- Filters the list by alert type: Help, Error, or Warning • **Connection Status**- Filters the list by connection status: In a Call, Online, or Offline • **Name** - Filters the list by system name entered • **IP Address** - Filters the list by IP address entered • **Alias** - Filters the list by the alias entered • **Site** - Filters the list by site location entered
Status	The state of the network device. Possible values include: • Online  • Offline  • In a call  • Unknown  • Device alert  • Gatekeeper registration error 
Name	The system name of the network device
Type	The type of network device. For valid device types, see "Network Device Types" on page 139.
IP Address	The IP address assigned to the network device
Site	The site to which the network device belongs
Alias	The alias assigned to the network device

Commands in the Monitor View

Besides providing access to the network device views, the **Actions** section of the **Monitor View** may also include these context-sensitive commands depending on the selected device type.

Command	Use this command to ...
Available for all device types	
Add	Manually add a network device to the Polycom CMA system or find a network device on the network
View Details	Display all of the **Device Details** for the selected network device
Edit	Change connection settings for the selected network device. Note that if this is a managed device, the device may overwrite settings entered manually.
Delete	Delete the selected network devices
Available for only selected network device types	
Manage	Open the selected network device's management interface in a separate browser window. This command is not available for the following device types: **MGC**, **GW/MCU**, and **Other**.

VBP View

Use the **VBP View** to manage Polycom Video Border Proxy™ (VBP™) firewall devices on the network.

Polycom VBP devices, when installed at the edge of the operations center, secures critical voice, video, and data infrastructure components including VoIP softswitches, video gatekeepers, gateways, media servers, and endpoints.

The **VBP** list has the following information.

Field	Description
Name	A unique name to identify the Polycom VBP device
Model	The model of Polycom VBP device
Provider-side IP	The private network IP address for the Polycom VBP device
Subscriber-side IP	The public network IP address for the Polycom VBP device

MCU View

Use the **MCU View** to manage Polycom MCU conferencing platforms on the network.

The **MCU** list has the same fields as the **Network Device > Monitor** view. For more information, see "Monitor View" on page 141.

DMA View

Use the **DMA View** to manage Polycom® Distributed Media Application™ (DMA™) systems on the network.

The Polycom DMA system uses advanced routing policies to distribute audio and video calls across multiple Polycom RMX media servers. It essentially acts like a single large MCU, greatly simplifying video conferencing resource management and improving efficiency.

Logically, the Polycom DMA system is a cooperative active/active two-node cluster. Both nodes can be actively registered with the gatekeeper and can accept and process calls.

If the Polycom CMA system is the gatekeeper, the system recognizes the H.323 gatekeeper registration requests from the DMA nodes to be part of a two-node cluster, but each node is registered individually. When both nodes are registered and the systems completely configured, the Polycom CMA system routes calls destined for the Polycom DMA system to the first node that it finds available. If the first node isn't available, it automatically routes the call to the second node.

You can also manually add DMA nodes to a Polycom CMA system.

Once the two nodes are registerd to a Polycom CMA system, finish the integration of the Polycom DMA system by completing the following tasks:

- Add the logical Polycom DMA system, as described in ...
- Change the **Available to Schedule** setting for the RMX media servers that the Polycom DMA system incorporates. See ...

In this initial release, a Polycom CMA system does not provide provisioning, softupdate, monitoring, alerts or control for a Polycom DMA system.

The **DMA** list has the following information.

Field	Description
Name	A unique name for the Polycom DMA system
Virtual IP Address	The virtual IP address for the Polycom DMA system
H.323 Alias	The alias used to identify both nodes in the Polycom DMA system
Description	A userful description for the Polycom DMA system

Device Gatekeeper Registration Policies

If the Polycom CMA system gatekeeper registration policy allows devices to register automatically (that is, a primary gatekeeper setting of **Allow Registration of All Endpoints**, **Allow Registration of Endpoints in Defined Sites**, or **Allow Registration of Endpoints with Defined E.164 Prefixes**), those registered devices are automatically added to the either the endpoint list or the network device list.

If the Polycom CMA gatekeeper registration policy does not allow devices to register automatically (i.e., a gatekeeper setting of **Allow Registration of Predefined Endpoints Only**), you must manually add all devices to the Polycom CMA system.

No matter what the gatekeeper registration policy, any device that is automatically provisioned, any device that is registered with the Global Address Book, and any device that is added manually to the Polycom CMA system can automatically register with the gatekeeper.

Note

You can also manually add devices to the Polycom CMA system for monitoring purposes only.

For more information, see "Device Registration" on page 242.

Cascading MCUs

To enable multi-bridge conferences, you must complete the following steps:

1. Configure entry queues on the participating MCUs. Only bridges with entry queues are display in the list of available bridges to schedule on the people-to-bridge or bridge-to-bridge scheduling screen.
2. Configure **MCU Cascading** for each bridge on the Polycom CMA system by editing each MCU and referencing the appropriate entry queue ID and ISDN numbers.

Some notes about cascading MCUs:

- A Polycom RMX 1000 MCU cannot be used for cascading.
- All devices (MCUs and endpoints) in a cascaded conference must be registered to the same Polycom CMA system gatekeeper.
- All systems (the Polycom CMA system, MCUs, and endpoints) must be time synchronized.

Configuring Cascading on a Polycom MGC MCU

When using a Polycom MGC MCU for cascading, version 8.0.2 or greater is required. Polycom recommends creating a cascade entry queue on every Polycom MGC MCU on the network.

To create a cascade entry queue on a Polycom MGC system, create an **Entry Queue Service** that has the **Cascade** check box enabled. If the cascade link is to be IP only, check the **IP Only** checkbox under **Target Conferences**. If the cascade link is to support ISDN, leave this box unchecked and configure the dial-in numbers. Also, enable the **Use Entry Queue** selection.

See the *Polycom MGC Manager User Guide* for additional information on configuring entry queues on a Polycom MGC system.

Configuring Cascading on a Polycom RMX 2000 MCU

When using a Polycom RMX 2000 MCU for cascading, Polycom recommends version 3.0 or greater. Earlier versions may cause a tunneling effect.

To configure cascading using a Polycom RMX 2000 MCU, you must create two cascading entry queues—one for which the **Master** option on the **Cascade** menu is selected and one for which the **Slave** option on the **Cascade** menu is selected. Also, enable the **Use Entry Queue** selection.

The primary purpose for the Master and Slave designation is to determine which Polycom RMX 2000 MCU is responsible for managing People+Content for the conference.

However, since ISDN cascade links on Polycom RMX MCUs are not supported, do not select **Enable ISDN/PSTN Access**. The Polycom CMA system only supports cascaded IP links on Polycom RMX 2000 MCUs. It does not support cascaded ISDN links on Polycom RMX 2000 MCUs.

Also, Polycom RMX systems enforce a 1x1 layout for the cascaded link between bridges, so only one participant on each bridge is displayed at any time. To change this on a Polycom RMX system v 4.0, go to **Setup > System Configuration** and on the **MCMS_PARAMETERS_USER** page add a new flag called `FORCE_1X1_LAYOUT_ON_CASCADED_LINK_CONNECTION` with a **Value** of `NO`.

This flag cannot be changed on Polycom RMX system v 3.x system.

13

MCU Bridge Management Operations

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA™) system MCU bridge management tasks. It includes these topics:

View Device Details

To view detailed information about a managed MCU bridge

1. Go to **Network Device > MCUs**.
2. As needed, use the **Filter** to customize the MCU list.
3. Select the MCU of interest and click **View Details** .

   The **Device Details** dialog box for the selected MCU appears.

Field	Description
Identification	
System Name	The name of the MCU. • MCU names must be unique. • The name must be in ASCII only[a] and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. • When retrieved from the MCU, the name is taken from the H.323 ID if the MCU registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.
Device Type	The type of MCU. For valid types, see "Network Device Types" on page 139.
IP Address	The assigned IP address of the MCU
Site	The network site for the MCU. By default, MCUs are added to the **Primary Site**.
Product ID	
Description	A free-form text field (Extended ASCII only[a]) in which information about the MCU can be added
Serial Number	The serial number (ASCII only[a]) of the MCU.The MCU provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the MCU (ASCII only[a]). The MCU provides the version number if it registered successfully or is managed.
HTTP URL	(RMX MCUs only) The management URL for the endpoint, if available (ASCII only[a]). This URL allows the Polycom CMA system to start the endpoint 's management system using the **Manage** function. All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the Polycom CMA system. For third-party endpoints that do not register using an IP address, you must enter the URL.
HTTP Port	(RMX MCUs only) The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.

Field	Description
Addresses	
DNS Name	The DNS name for the MCU
Aliases	The aliases that allow you to connect to the MCU. The Polycom CMA system converts the aliases to the IP address associated with the MCU. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown. • The value for the H.323 ID is the MCU name if the MCU registered with the gatekeeper and it is a third-party system. In other cases, the MCU name is the system name, which might be different from the H323 ID. **Note** The following **Alias Values** are ASCII only[a]: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.
ISDN Video Number	The country code + city/area code + phone number for the MCU.
Capabilities	
Supported Protocols	The communications protocols that the MCU can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. The MCU automatically provides the protocols if it registered successfully or is managed.
Capabilities Enabled	Capabilities to enable on this MCU. Options are: • **MCU** - The device can act as a control unit for multipoint conferences • **Gateway** - (MGC MCUs only) The device can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed.
Available to Schedule	Select this option to make the MCU available when users are scheduling conferences
Monitoring Level	The monitoring level for the MCU. Possible values include: • **Standard.** This MCU is monitored. • **VIP.** This MCU is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.

Field	Description
MCU Services	
Service Type	The available network services may include: • **H.323 Service**—Indicates a connection to an IP network using the H.323 protocol. • **H.320 Service**—Indicates a connection to an ISDN phone line using the H.320 protocol. • **Gateway Service**—(MGC MCUs only) Indicates a connection to both IP and ISDN to enable conversion from one protocol to the other. Direct Service--Indicates a direct connection between an MCU and a video endpoint system, using a serial cable.
Service Name	
Priority	
MCU Resources	
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	(RMX MCUs only)
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.
Max Transcoding Ports	(MGC MCUs only) Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a meeting.
Max Voice Ports	
Max CP Resolution	
Max Bandwidth Capacity (Kbps)	
Alerts (RMX MCUs only)	
Category	
Level	
Code	
Card Alerts (MGC MCUs only)	

Field	Description
Slot	
Type	
Errror	
Warning	

a. For more information on field limitations, see "Field Input Requirements" on page 6.

Add an MCU Manually

This section describes how to add an MCU to a Polycom CMA system.

Note

Back-end communication with the RMX control units and IP service blades must be enabled.

When you add an MCU device, MCU services are added automatically at the time the IP card registers with the Polycom CMA system.

When you add a gateway device, use the **Services** screen to specify the network services available for the device.

Notes

- Polycom RMX 2000 devices may only have H.323 service.
- Once an MCU registers with the Polycom CMA system, if you change an MCU service on the MCU, the update does not automatically get sent to the Polycom CMA system. To update the system, you must delete and readd the MCU to the system.
- These network services are not the same as the **Dial Plan Services** such as **Simplified Dialing** and **Conference on Demand**. Network services describe the physical connection that the device supports. Dial plan services provide access to specific features used for routing calls by dialing a prefix.

When you enter network service information manually, remember that the Polycom CMA system does not create the service at the device. The service must have already been defined at the device. Enter information in the Polycom CMA system that matches the information in the device.

If you do not define network services, you may not use an MCU or gateway in a conference. For example, if you do not define the H.323 service on the MCU, when the Polycom CMA system tries to schedule a video conference that requires this service, it will look for another MCU with this service. If another MCU with this service is not available, the conference will not be scheduled.

To add an MCU bridge to a Polycom CMA system or find an MCU on the network

1. Go to **Network Device > MCUs** and click **Add**  .
2. In the **Add New Device** dialog box, select the **Device Type** of interest. For valid types, see "Network Device Types" on page 139.
3. Enter the **IP Address** of the MCU.
4. Enter the **Admin ID** and **Password** for the MCU.
5. Click **Find Device**.
   - If the Polycom CMA system can find the MCU on the network, the **Add New Device** dialog box is populated with information retrieved from the MCU. Review any information retrieved from the MCU.
   - If the Polycom CMA system cannot find the MCU on the network, a **Device Not Found** dialog box appears.
6. Click **OK**.
7. Complete the **Identification**, **Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading** sections of the **Add New Device** dialog box. (For more information, see "View Device Details" on page 147.) At a minimum, assign the MCU a **System Name**.

   Pay particular attention to the **Capabilities** options, because the settings on it determine how the MCU is used throughout the Polycom CMA system.

   Note that many fields in this dialog box are ASCII only. For more information, see "Field Input Requirements" on page 6.
8. Click **Add**.

   The MCU appears in the **Network Device** list. By default, the system:
   - Adds the MCU to the applicable site
   - Sets the **HTTP Port** to 80
   - Adds an **Alias** for the endpoint
   - Makes the endpoint **Available to Schedule**
   - Sets the **Monitoring Level** to **Standard**

Notes

- In the **Device List**, a Polycom CMA system displays a single MCU as two separate **Device Types** (an **RMX** or **MGC** device and a **GW/MCU** device). The GW/MCU designation represents the network interface.
- For third-party endpoints, the HTTP URL, serial number, and DNS name are not captured during endpoint registration.

Edit an MCU Bridge

To edit an MCU from the Polycom CMA system

1. Go to **Network Device > MCUs**.
2. As needed, use the **Filter** to customize the MCU list.
3. Select the MCU of interest and click **Edit** .
4. Complete the **Identification**, **Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading** sections of the **Edit Device** dialog box. (For more information, see "View Device Details" on page 147.) At a minimum, assign the MCU a **System Name**.
5. Click **Update**.

Enable Cascading Conferences

To enable cascading conferences

1. On the MCUs, configure entry queues as required and record the entry queue number(s). For more information, see "Cascading MCUs" on page 144 or the product documentation for the MCU.
2. Go to **Network Device > MCUs**.
3. As needed, use the **Filter** to customize the MCU list.
4. Select the MCU of interest and click **Edit** .
5. Go to the **MCU Resources** section of the **Edit Device** dialog box and select **Use Entry Queue**.
6. Go to the **MCU Cascading** section of the **Edit Device** dialog box.
7. For a Polycom RMX 2000 MCU:
   a. Enter the **Master Entry Queue Number ID** and **Slave Entry Queue Number ID**.
   b. (Optional) Enter the **Master Entry Queue ISDN Number** and **Slave Entry Queue ISDN Number.**
8. For a Polycom MGC MCU:
   a. Enter the **Cascade Entry Queue Number ID**.
   b. (Optional) Enter the **Cascade Entry Queue ISDN Number.**
9. Click **Update**.

Delete an MCU Bridge

To delete an MCU from the Polycom CMA system

1. Go to **Network Device > MCUs.**
2. As needed, use the **Filter** to customize the MCU list.
3. Select the MCU of interest and click **Delete** .
4. Click **Yes** to confirm the deletion.

   The **MCU** list is updated.

View Bridge Hardware

To view the hardware configuration of a bridge:

1. Go to **Network Device > Bridge View**.

   As needed, use the filter to customize the bridge list.
2. In the bridge list, select the bridge of interest and click V**iew Hardware**.

   A **Hardware** pane appears below the bridge list. It lists the hardware for the selected bridge and displays the **Slot number**, **Card Type**, **Status**, **Temperature**, and **Voltage** for each piece of hardware.

View Bridge Services

To view the services available on the bridge:

1. Go to **Network Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Services**.

   A **Services** pane appears below the bridge list. It lists the services for the selected bridge and identifies the **Service Type**, **Service Name**, and the default setting for the service.

View Bridge Conferences

To view information about the conferences resident on the bridge:

1. Go to **Network Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Conferences**.

   A **Conferences** pane appears below the bridge list. It lists the conferences for the selected bridge and identifies the conference **Status**, **Type**, **Name**, **Start Time**, **Bridge**, and **Owner**.

View Bridge Ports

To view information about the bridge ports:

1. Go to **Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Ports**.

   A **Ports** pane appears below the bridge list. It lists the ports for the selected bridge and identifies the **Audio Ports Available**, **Video Ports Available**, **Audio Ports in Use**, and **Video Ports in Use**.

View Bridge Meeting Rooms

To view information about meeting rooms on a bridge:

1. Go to **Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Meeting Rooms**.

   A **Meeting Rooms** pane appears below the bridge list. It lists the meeting rooms for the selected bridge and identifies the meeting room by **Name**, **ID**, **Duration**, **Conference**, **Chairperson**, **Profile**.

View Bridge Entry Queues

To view information about entry queues on a bridge:

1. Go to **Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Entry Queues**.

   An Entry Queues pane appears below the bridge list. It lists the entry queues for the selected bridge and identifies the entry queue by **Name**, **ID**, **Profile**, and **Dial-In Number**.

View Bridge Gateway Conferences

To view information about gateway conferences on a bridge:

1. Go to **Device > Bridge View**.
2. As needed, use the filter to customize the bridge list.
3. In the bridge list, select the bridge of interest and click **View Gateway Conferences**.

   If the feature is available on the bridge, a Gateway Conferences pane appears below the bridge list. It lists the gateway conferences for the selected bridge.

14

Management Operations for Other Network Devices

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA™) system network device management tasks. It includes these sections:

- Polycom VBP Management Operations
- Polycom DMA Management Operations

Polycom VBP Management Operations

The Polycom Video Border Proxy device management operations include these topics:

- Add a Polycom Video Border Proxy Device
- Edit a Polycom Video Border Proxy Device
- Delete a Polycom Video Border Proxy Device
- Identify Endpoints Using the Polycom Video Border Proxy Device
- Identify Endpoints Using the Polycom Video Border Proxy Device

Add a Polycom Video Border Proxy Device

To add a Polycom Video Border Proxy (VBP) device to a Polycom CMA system

1 Go to **Network Device > VBPs** and click **Add**  .

2 Configure these settings in the **Add VBP** dialog box.

Column	Description
Name	A unique name to identify the Polycom VBP device

Column	Description
Provider-side IP	The Private Network IP address for the Polycom VBP device
Subscriber-side IP	The Public Network IP address for the Polycom VBP device

3 Click **OK**.

The Polycom VBP device is added to the Polycom CMA system. However, more configuration may be necessary for the device to operate in your network. See the product documentation for the device.

Edit a Polycom Video Border Proxy Device

To edit a Polycom Video Border Proxy (VBP) device

1 Go to **Network Device > VBPs**

2 Select the Polycom VBP device of interest and click **Edit**  .

3 Configure these settings as needed in the **Edit VBP** dialog box.

4 Click **OK**.

Delete a Polycom Video Border Proxy Device

To delete a Polycom Video Border Proxy (VBP) device from a Polycom CMA system

1 Go to **Network Device > VBPs**.

2 Select the Polycom VBP device of interest and click **Delete**  .

3 Click **Yes** to confirm the deletion.

Identify Endpoints Using the Polycom Video Border Proxy Device

Note

This procedure identifies only Polycom HDX and CMA Desktop systems that are:

- Registered to the Polycom CMA system
- Using the Polycom VBP firewall
- Operating in dynamic management mode.

One Polycom HDX or legacy endpoint system operating in standard management mode, registered to the Polycom CMA system, and using the Polycom VBP firewall may also be displayed in the **Endpoint** list. This entry may represent multiple endpoints, since all Polycom HDX or legacy endpoint system operating in standard management mode register with the same information..

To identify which endpoints are using the Polycom Video Border Proxy (VBP) firewall

1. Go to **Endpoint > Monitor View**.
2. Click **Select Filter** and select **IP Address**.
3. Enter the provider-side IP address of the Polycom VBP device and press **Enter**.

   The **Endpoint** list displays the dynamically-managed endpoints that are registered to the Polycom CMA system and using the Polycom VBP firewall.

Polycom DMA Management Operations

The Polycom Video Border Proxy device management operations includes these topics:

- Add Polycom DMA System Nodes
- Edit a Polycom DMA System
- Delete a Polycom DMA System

Add Polycom DMA System Nodes

To add Polycom DMA system nodes to a Polycom CMA system

1. Go to **Network Device > Monitor View** and click **Add**  .
2. In the **Add New Device** dialog box, select the **DMA node**.
3. Enter the **IP Address** of the DMA node to add.

4 Enter the **Admin ID** and **Password** for the DMA node.

5 Click **Find Device**.

- If the Polycom CMA system can find the DMA node on the network, the **Add New Device** dialog box is populated with information retrieved from the node. Review any information retrieved from the node.
- If the Polycom CMA system cannot find the DMA node on the network, a **Device Not Found** dialog box appears.

6 Click **OK**.

7 Complete the **Identification**, **Addresses,** and **Capabilities** sections of the **Add New Device** dialog box. At a minimum, assign the DMA node a **System Name** and an **Alias**.

Note that many fields in this dialog box are ASCII only. For more information, see "Field Input Requirements" on page 6.

8 Click **Add**.

The DMA node appears in the **Network Device** list.

9 Repeat steps 1 through 8 for the second DMA node. Once both nodes are added to the Polycom CMA system, you can continue on "Add a Polycom DMA System" on page 161.

Add a Polycom DMA System

To add a Polycom DMA system to a Polycom CMA system

1 Go to **Network Device >Monitor View** and verify that both DMA nodes for the cluster are added to the Polycom CMA system.

To add a Polycom DMA system to the Polycom CMA system, both nodes of a Polycom DMA cluster must be registered with the system. If the nodes are not registered with the Polycom CMA system, you can add them manually and then add the system. See "Add Polycom DMA System Nodes" on page 159.

2 Once both nodes are listed, go to **Network Device > DMAs** and click **Add**  .

3 Configure these settings in the **Add DMA** dialog box.

Column	Description
Name	A unique name for the Polycom DMA system
Description	A userful description for the Polycom DMA system
Virtual IP Address	The virtual IP address for the Polycom DMA system
Admin ID	The administrator ID for the Polycom DMA system
Admin/Confirm Password	The administrator password for the Polycom DMA system
H.323 Alias	The alias used to identify both nodes in the Polycom DMA system

4 Click **Add**.

The Polycom DMA system is added to the Polycom CMA system. However, more configuration may be necessary for the DMA system to operate in your network. See the product documentation for the DMA system.

Edit a Polycom DMA System

To edit a Polycom DMA system

1 Go to **Network Device > DMAs.**

2 Select the Polycom DMA system of interest and click **Edit**  .

3 Configure these settings as needed in the **Edit DMA** dialog box.

Column	Description
Name	A unique name for the Polycom DMA system
Description	A userful description for the Polycom DMA system
Virtual IP Address	The virtual IP address for the Polycom DMA system
Admin ID	The administrator ID for the Polycom DMA system
Admin/Confirm Password	The administrator password for the Polycom DMA system
H.323 Alias	The alias used to identify both nodes in the Polycom DMA system

4 Click **OK**.

Delete a Polycom DMA System

To delete a Polycom DMA system from a Polycom CMA system

1 Go to **Network Device > VBPs**.

2 Select the Polycom DMA system of interest and click **Delete**  .

3 Click **Yes** to confirm the deletion.

15

MCU Bridge Device Details

This chapter lists the fields found in the MCU Device Detail section of the Polycom® Converged Management Application™ (CMA™) system interface. It includes these sections:

MCU H.320 Services

Field	Description
MCU H.32O Service	
Service Name	Name of the H.320 ISDN service
Channels	Number of 64K channels dedicated to the MCU
Number Range	Dial-in number range of service. These ISDN numbers are available on an MCU for all endpoints to use. Also called direct inward dialing (DID).
LCR Table	The least-cost routing table for calls made through this gateway
Local Prefix	The prefix required to place a call to a local number outside the enterprise. For example, if you dial 9 to reach an outside line, the Local Prefix is 9.
Non-Local Prefix	The prefix required to dial long distance. For example, in certain states in the United States, you must dial 1 before you can dial a non-local number.

Field	Description
International Prefix	The prefix required to dial an international number. For example, in many countries, the international prefix is 00.
Local Area Code	A list of local area codes, separated by commas
Priority	The priority order for this service

MCU H.323 Services

Field	Description
Service Name	The name of the H.323 service (ASCII only[a]) defined in the MCU.
Dialing Prefix	Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.
Service IP Address	IP address associated with this network service and with this H.323 card in the MCU.
Alias	Alias for the service defined in the MCU. **Note** Polycom recommends using E.164 as the alias for this service. The number that is dialed if the endpoints are registered with the same gatekeeper. If the endpoints are not registered with the same gatekeeper, they use their assigned IP address to connect.
Port	Number of IP connections available.
Priority	The priority order for this service.

a. For more information, see “Field Input Requirements” on page 6.

MCU Gateway Services

Field	Description
Service Name	The name of the H.323 service defined in the MCU.
Dialing Prefix	Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.

Field	Description
H320 Service Name	Select a defined H320 service
Channels	Number of 64K channels dedicated to the MCU.
Priority	The priority order for this service.

MCU Resources—Polycom MGC Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.
Max Transcoding Ports	Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Total IP Parties (Embedded MCU devices)	Maximum number of IP calls that can be made from this endpoint.
Total ISDN Parties (Embedded MCU devices)	Maximum number of ISDN calls that can be made from this endpoint.
Total Transcoded Parties (Embedded MCU devices)	Maximum number of transcoded calls (IP and ISDN calls combined) that can be made from this endpoint.
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a meeting.
Entry Queue ISDN Number	The ISDN-allocated phone number of the IVR. ISDN devices only.

MCU Resources—Polycom RMX 2000 Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	Maximum number of video ports on which participants can be connected.
Max Licensed Video Ports	Maximum number of total video participants allowed at once on this MCU.

Field	Description
Use Entry Queue	Indicates whether the RMX 2000 device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a meeting.
Audio & Video Settings: The following parameters must be set manually to synchronize the with the RMX 2000 device. See the RMX 2000 documentation for more information about these settings.	
RMX API Version	Choose Pre-2.0 if you have an RMX 1.x system. Choose 2.0 or greater if you have an RMX 2.x system.
Max Voice Ports	Only available when RMX API Version is 2.0 or greater. Set this to the maximum number of audio ports configured on the RMX device. Refer to the *RMX 2000 Administrator's Guide* for more information about this field. **Note** Up to 10 blocks of RMX video ports can be converted to 50 audio-only ports, up to a maximum of 200 audio-only ports.
Max CP Resolution	Only available when **RMX API Version** is 2.0 or greater. Set this to the highest available video format. Choices are: None, CIF, SD15, and SD30. Refer to the *RMX 2000 Administrator's Guide* for more information about this field.

16

Users and Groups Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) system users and groups management structure. It includes these topics:

Groups, Users, and User Roles

The Polycom CMA system allows an administrator with **System Setup** permissions to manage users, groups, user roles, and permissions. Most often a Polycom CMA system is integrated with an enterprise directory from which users are imported. However, the Polycom CMA system also allows an administrator with **System Setup** permissions to add local users (i.e., users added manually to the system) and associate them with devices and roles.

Users

Local Users

When you manually add local users, the Polycom CMA system manages all user information and associations.

At a minimum, when you manually add users, you must enter a user's **First Name** or **Last Name**, **User ID**, and **Password**. When you enter the minimum information, the Polycom CMA system automatically assigns local users the basic **Scheduler** role. They can then schedule conferences, be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with devices.

You should associate local users with one or more roles and associate them with one or more devices. Alternatively, you can associate local users with roles by associating them with local groups.

Enterprise Users

When the Polycom CMA system is integrated with an enterprise directory, the Polycom CMA system manages only three pieces of an enterprise users' information: the devices, roles, and alert profiles assigned to them. The remaining information is pulled from the enterprise directory.

Notes

- Currently, the Polycom CMA system supports only a Microsoft Active Directory implementation of an LDAP directory.
- You cannot have more than 18 users with the same first and last name in the Polycom CMA system, and their user IDs must be unique across all users and rooms and across all domains.

When the Polycom CMA system is integrated with an enterprise directory, users imported into the system through the enterprise directory are by default added to the system without a role. This default set up allows users to log into the Polycom CMA system with their enterprise user IDs and passwords. They can then be scheduled into conferences and call into conferences. However, the system cannot call out to them until they are associated with devices.

To be fully functional, you must associate enterprise users with one or more roles to control their access to system functions and associate them with one or more devices. Alternatively, you can associate enterprise users with roles by associating them with local or enterprise groups.

If you want the Polycom CMA system to, by default, automatically assign enterprise users the basic **Scheduler** role, you must change the appropriate system **Security Settings**. See "Change the Default User Access to the Polycom CMA System" on page 283.

Groups

Groups provide a more efficient and consistent use of the Polycom CMA system , because they allow you to assign roles and provisioning profiles to sets of users rather than to individual users.

Local Groups

The Polycom CMA system allows you to add local groups (i.e., groups added manually to the system) and associate them with with provisioning profiles and roles.

For local groups, the Polycom CMA system manages all group information and associations. The following table shows the group information that the Polycom CMA system maintains.

Enterprise Groups

When the Polycom CMA system is integrated with an enterprise directory, groups defined to the enterprise directory are not automatically added to the Polycom CMA system, but you can import them into the system.

When the Polycom CMA system is integrated with an enterprise directory, the system manages only three pieces of group information: the provisioning profile assigned to the group, the roles assigned to the group, and whether or not the group is Directory Viewable (i.e., displayed in endpoint directories). The remaining group information is pulled from the enterprise directory.

For system and endpoint directory performance purposes, two best practices in regards to enterprise groups are:

- Do not import more than 500 enterprise groups into a Polycom CMA system
- Do not mark more than 200 enterprise groups as Directory Viewable

Roles and Permissions

The Polycom CMA system is a role and permissions based system.

- Users are assigned one or more user roles either directly or through their group associations
- User roles are assigned a set of permissions
- Users see only the pages and functions available to their roles and associated permissions. Permissions are cummulative, so users see all of the pages and functions assigned to all of their roles.

Note

Users inherit roles from their parent groups—local or enterprise. They cannot inherit roles from groups more distantly removed—for example, from their grandparent groups.

An administrator has several options when implementing user roles.

1. Implement only the system default user roles of **Administrator**, **Operator**, and **Scheduler** and keep the standard permissions assigned to these roles.

2 Implement only the system default user roles of **Administrator**, **Operator**, and **Scheduler** but change the permissions assigned to the **Operator**, and **Scheduler** roles.

> **Note**
> To ensure Polycom CMA system access and stability, the default roles cannot be deleted and the Administrator role cannot be edited.

3 Implement either option 1 or 2, but also create additional unique, workflow-driven user roles and determine which permissions to assign to those user roles.

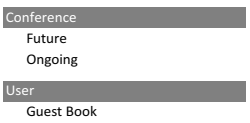
As a best practice, we recommend you create an **Advanced Scheduler** role and associate it with just advanced scheduling permissions.

Some important notes about user roles and permissions:

- Users (local and enterprise) may be assigned more than one role. In this case, the permissions associated with those roles are cummulative; a user has all of the permissions assigned to all of his roles.
- Users (local and enterprise) may be assigned roles as an individual and as part of a group. Again, the permissions associated with those roles are cummulative; a user has all of the permissions assigned to all of his roles no matter how that role is assigned.
- Users assigned a role with any one of the **Administrator Permissions** are generally referred to as administrators. Users assigned a role with any one of the **Operator Permissions** and none of the **Administrator Permissions** are referred to as **Operators**. Users assigned a user role with **Scheduler Permissions** and none of the **Administrator** or **Operator Permissions** are referred to as **Schedulers**.

Scheduler Role, Permissions, and Functions

A scheduler who is assigned the default Scheduler role with the default permissions has access to the following functions:



Operator Role, Permissions, and Functions

An operator who is assigned the default operator role with the default permissions has access to the following functions:

- **Conference**
  - Ongoing
- **Endpoint**
  - Monitor View
- **Network Device**
  - Monitor View
  - VBPs
  - MCUs
  - DMAs
- **User**
  - Guest Book
- **Reports**
  - IP Call Detail Records
  - ISDN Call Detail Records
  - Endpoint Usage Report
  - Gatekeeper Message Log

Administrator Role, Permissions, and Functions

An administrator who is assigned the default administrator role with the default permissions has access to the following functions:

- **Conference**
  - Future
  - Ongoing
- **Endpoint**
  - Monitor View
  - Automatic Provisioning
  - Scheduled Provisioning
  - Automatic Softupdate
  - Scheduled Softupdate
- **Network Device**
  - Monitor View
  - VBPs
  - MCUs
  - DMAs
- **User**
  - Users
  - Groups
  - User Roles
  - Guest Book
- **Reports**
  - Site Statistics
  - Site-Link Statistics
  - IP Call Detail Records
  - ISDN Call Detail Records
  - Endpoint Usage Report
  - Conference Summary Report
  - Gatekeeper Message Log
  - System Log Files
- **Admin**
  - Dashboard
  - Conference Templates
  - Conference Settings
  - Provisioning Profiles
    - Automatic Provisioning Profiles
    - Scheduled Provisioning Profiles
  - Software Updates
    - Automatic Software Updates
    - Scheduled Software Updates
  - Rooms
  - Global Address Book
  - Server Settings
    - Network
    - System Time
    - Database
    - LDAP
    - Licenses
    - Redundant Configuration
    - Custom Logo
    - Global Address Book
    - Remote Alert Setup
    - E-mail
  - Gatekeeper Settings
    - Primary Gatekeeper
    - Alternate Gatekeeper
    - Neighboring Gatekeepers
- **Admin (continued)**
  - Management and Security
    - Server Software Upgrade
    - Certificate Settings
    - Security Settings
    - Endpoint Management Settings
  - Dial Plan and Sites
    - Sites
    - Site-Links
    - Site Topology
    - Services
    - Dial Rules
    - LCR Tables
  - Alert Settings
    - CMA Alert Level Settings
    - Endpoint Alert Level Settings
    - Remote Alert Profiles
  - Database Backup Files

Device Associations and Presence

The Polycom CMA system assumes that users will be associated with devices. You can associate a user with more than one device, but one device is designated as the primary device.

When scheduling a user in a conference, the Polycom CMA system will, by default, schedule the user's primary device. The scheduler can choose to change the request to schedule one of the user's other devices.

The Polycom CMA system is also a presence service, which is the part of the system that maintains online status information for the users of dynamically managed devices. The presence service allows users to access information about the online status of other users. This is important, because when you make a video call or start a chat, that action only takes you to a device. It doesn't ensure that you will reach the person you want to reach. The presence service provides information about the user's availability, which improves your chances of getting the person.

User Management

The Polycom CMA system manages the following user, group, and room management entities:

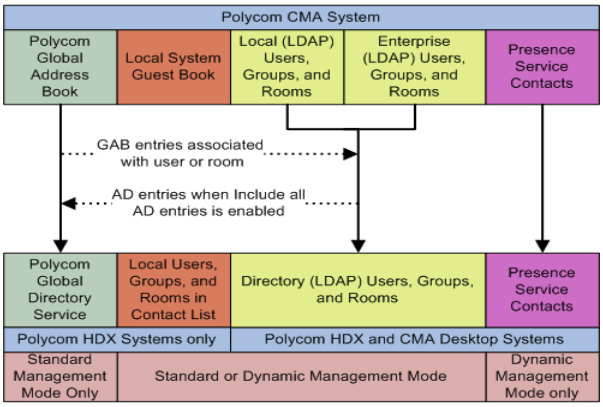
Name	Description	Comments
Users list	Displays local and enterprise user accounts. Local users are added to the system manually. Enterprise users appear in the **Users** list when you associate the Polycom CMA system with an enterprise directory.	For Polycom endpoint systems, such as Polycom HDX systems, these local and enterprise user, group, and room entries may appear in the endpoint's directory and/or contacts. For more information, see the endpoint system's product documentation
Groups list	Displays local and enterprise groups. Local groups are added to the system manually. Enterprise groups appear in the **Groups** list when you associate the Polycom CMA system with an enterprise directory and then import the enterprise groups.	
Rooms list	Displays local and enterprise rooms. Local rooms are added to the system manually. Enterprise rooms appear in the **Rooms** list when you associate the Polycom CMA system with an enterprise directory and then search for the room in the enterprise directory.	
Global Address Book	Automatically populated by devices that register with the gatekeeper function of the Polycom CMA system. You can edit a device in this list and associate the device with a user.	For Polycom endpoint systems, such as Polycom HDX systems, Global Address Book entries may appear in the endpoint's directory and/or contacts. For more information, see the endpoint system's product documentation Polycom CMA Desktop systems cannot access the Global Address Book.
System Guest Book	Entries added to the system Guest Book when Polycom CMA system schedulers enable the **Save to Guest Book** option when they add a guest participant to a conference.	The Guest Book is only available to people scheduling conferences via the Polycom CMA system Web Scheduler.
Presence service contacts	For dynamically-managed endpoint systems only. Presence service contacts are XMPP buddy entries saved as contacts by both buddies and stored with the presence service. Entries saved as contacts by both buddies and stored with the presence service share presence status.	Not listed in the Polycom CMA system interface. Stored in the system database as the `XMPP_db` file.

Some additional settings may affect whether or not entries appear in an endpoint's directory:

- When **Directory Viewable** is enabled for a local or enterprise group (the default setting), the group appears in the endpoint system's directory .

- When **Allow Directory Changes** is enabled at the endpoint, Polycom HDX systems can manage their own set of local and enterprise users, groups, and rooms or their own local contacts.
- When you can specify a default contact group (also called the **Default LDAP Group**), the members in this default contact group appear in the endpoint systems' contact list.

The following illustration shows the relationship between the Polycom CMA system user management entities and those of the dynamically managed endpoints.



17

User Management Operations

This chapter includes information on managing users and groups within the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Manage Users

In the Polycom CMA system, only administrators with **Directory Setup** permissions can view, add, edit or delete users.

Search for a User

To search for a user

1 Go to **User > Users** and in the **Search Users** field, enter the name for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.

Note
Searches for a user are case-insensitive, exact-match searches of the **Username**, **First Name**, and **Last Name** fields.

2 To search for a local user, press **Enter**.

3 To search both local and enterprise users, first clear the **Local Users Only** checkbox and then press **Enter**.

Note
If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.

4 If the list is too large to scan, further refine your search string.

Add a User

To add a user

1 Go to **User > Users**, and click **Add User**.

2 Configure the **General Info** section of the **Add New User** dialog box.

Column	Description
User ID	The user's unique login name. This user ID must be unique across all rooms and users and across all domains.
Password	The user's assigned password
First Name	The user's first name
Last Name	The user's last name
Domain	The domain associated with the user
Email Address	The user's email address. (The **Email** address is an ASCII-only field.[a]) **Note** The Polycom CMA system identifies plugin users and their associated devices by email address, so this is required information for the plugin to work.

a. For more information, see "Field Input Requirements" on page 6.

3 In the **Associated Devices** section, select and move the required device(s) to **Selected Devices** list. Move the unwanted device(s) to the **Available Devices** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.

4 In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list. Press **Shift-click** or **Ctrl-click** to select multiple items in the list.

Note
If the user has multiple devices, list the devices in order of priority, with the primary device first.

5 Click **OK**.

Edit a User

For users added manually to the Polycom CMA system, you can edit all user information except the user ID.

For users added through the enterprise directory, you can edit their roles (unless the role is inherited from a group) and associate them to devices, but you cannot change user names, user IDs, or passwords.

To edit a user

1 Go to **User > Users** and in the **Search Users** field, enter the name for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.

Note
Searches for a user are case-insensitive, exact-match searches of the **Username**, **First Name**, and **Last Name** fields.

2 To search for a local user, press **Enter**.

3 To search both local and enterprise users, first clear the **Local Users Only** checkbox and then press **Enter**.

Note
If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

4 If the list is too large to scan, further refine your search string.

5 Select the user of interest and click **Edit User**.

6 As required, edit the **General Info**, **Associated Devices,** and **Associated Roles** sections of the **Edit User** dialog box.

7 Click **OK**.

Delete a User

You can only delete local users from the Polycom CMA system. You cannot delete users added through integration with an enterprise directory.

To delete a user

1 Go to **User > Users** and in the **Search Users** field, enter the name for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.

> **Note**
> Searches for a user are case-insensitive, exact-match searches of the **Username**, **First Name**, and **Last Name** fields.

2 To search for a local user, press **Enter**.

3 To search both local and enterprise users, first clear the **Local Users Only** checkbox and then press **Enter**.

> **Note**
> If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

4 If the list is too large to scan, further refine your search string.

5 Select the user of interest and click **Delete User**.

6 Click **Yes** to confirm the deletion.

The user is deleted from the Polycom CMA system.

Manage Groups

Add a Local Group

To add a local group

1 Go to **User > Groups**.

2 In the **Groups** page, click **Add Local Group**.

3 Complete the **General Info** section of the **Add Local Group** dialog box.

Column	Description
General Info	
Group Name	A meaningful group name assigned when creating the group
Description	A more complete description of the group's purpose
Directory Viewable	Whether or not the group is displayed in the endpoint directory
Provisioning Profile	The automatic provisioning profile assigned when creating the group
Associated Roles	
Available Roles	The list of roles defined to the CMA system
Selected Roles	The list of roles that you assign users when adding them to the system. Users have all of the permissions associated with all of the roles assigned to them (i.e., permissions are cummulative).
Group Members (Local Users Only)	
Search Available Members	Search field for finding users
Search Results	The users and groups identified to the system that you can add to the local group. This list can include both local and enterprise users and groups.
Group Members	The users and groups selected as part of the group

4 In the **Search Available Members** field of the **Group Members** dialog box, search for the users and groups to add to this local group. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.

5 In the **Search Results** section, select and move the users and groups of interest to the **Group Members** list. To select all users and groups listed, click the checkbox in the column header.

6 Click **OK**.

The group appears in the **Groups** list. It is identified as a LOCAL group.

Import Enterprise Groups

To import one or more enterprise groups

1 Go to **User > Groups**.

2 In the **Groups** page, click **Import EnterpriseGroup**.

3 In the **Search Available Groups** field of the **Import EnterpriseGroup** dialog box, type all or part of the group name (with wildcards) and press **ENTER**. For example, to search for Print Operator, enter Pri* or *Op*.

Note

Searches for a group are case-insensitive, exact-match searches of the **Group Name** field. Use wildcard characters to perform substring searchs.

4 In the **Search Results** list, select the enterprise groups to add. To select all enterprise groups, click the checkbox in the column header.

5 Click the right arrow to add the enterprise groups to the **Groups to Import** list.

6 Click **OK**.

The enterprise group appears in the **Groups** list. Now you can edit the group and associate it with an automatic provisioning profile, user roles, and specify whether or not the group directory is viewable.

Edit a Group

To edit a local or enterprise group

1 Go to **User > Groups**.

2 In the **Groups** page, select the group of interest and click **Edit Group**.

3 As required, edit the **General Info**, **Associated Roles,** and **Group Members** sections of the **Edit Local Groups** dialog box.

Notes

- The **Group Members** section is only available for Local groups.
- If you remove a user from a group or a role from a group, the user no longer has the roles associated with the group.

4 Click **OK**.

Delete a Group

To delete a local or enterprise group

1 Go to **User > Groups**.

2 In the **Groups** page, select the group of interest and click **Delete Group**.

3 Click **Yes** to confirm the deletion.

The group is deleted from the Polycom CMA system.

Note

An enterprise group is only deleted from the Polycom CMA system, not the enterprise directory, so it can be reimported.

Specify a Default Contact Group

For those endpoint systems that the Polycom CMA system dynamically manages, you can specify a default contact group (also called the **Default LDAP Group**). The members in this default contact group, which is sent to the dynamically managed endpoint systems at a site during automatic provisioning, appear in the endpoint systems' contact list.

To specify a default contact group

1 Go to **System Setup > Dial Plan and Sites > Sites**.

2 In the **Sites** list, select the site of interest and click **Edit Site Provisioning Details**.

3 Click **LDAP Settings**.

4 In the **LDAP Default Group** menu, select the local or enterprise group that you wish to specify as the default contact group.

5 Click **OK**.

The **Sites** list reappears. During the next automatic provisioning of the endpoint, the default contact group is provisioned.

Manage User Roles

Assign Users Roles and Devices

You can assign roles to both local and enterprise users and associate them with devices.

To assign a role and endpoint to a user

1 Go to **User > Users**.

2 To search for a user:

a In the **Search** field of the **Users** page, type a search string. For example, to search for Barbara Smythe enter Bar* or *Smy*.

Note
Searches for a user on the Polycom CMA system **Users** page are case-insensitive, exact-match searches of the **Username**, **First Name**, and **Last Name** fields.

b To search both local and enterprise users, clear the **Local Users Only** checkbox and press **Enter**.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.

c If the list is too large to scan, further refine your search string.

3 Select the user of interest and click **Edit**.

4 In the **Devices** section of the **Edit User** dialog box, select the device you want to associate with the user and move it to the **Selected Devices** column. If a user has multiple devices, the first device listed is the user's default device.

5 Click **Finish**.

View the List of User Roles

To view the list of User Roles

>> Go to **User > User Roles**.

The **User Roles** list appears. It can be filtered by **Name** and **Description**.

Column	Description
Name	The unique name of the user role
Description	An optional dscription of the role

Add a User Role

When you add a user role, you also specify permissions for the role.

To add a new user role

1. Go to **User > User Roles**.
2. On the **User Roles** page, click **Add Role**.
3. Complete the **Name** and **Description** fields of the **Add Role** dialog box and assign permissions to the new role.

   The following table describes the fields of the **Add Role** dialog box.

Field	Description
Name	The unique name (ASCII only[a]) of the user role
Description	(Optional) A userful description (ASCII only[a]) of the user role
Administrator Permissions	Identifies which Polycom CMA system administrator pages and functions are available to the user role.
Operator Permissions	Identifies which Polycom CMA system operator pages and functions are available to the user role.

Field	Description
Scheduler Permissions	Identifies which Polycom CMA system scheduling pages and functions are available to the user role. **Scheduling Level.** This setting determines the level of scheduling available through this role. Possible values are: • **Basic.** Users can schedule conferences using the conference templates defined for them. They cannot access or edit the advanced **Conference Settings**. • **Advanced.** Users can schedule conferences using the conference templates defined for them. They can also access and edit the advanced **Conference Settings**.

a. For more information, see "Field Input Requirements" on page 6.

4 Click **Save**.

The new user role appears in the Polycom CMA system.

Edit Permissions for a User Role

You can change permissions for the default **Operator** and **Scheduler** roles, as well as for other user roles that were created manually. You cannot change permissions for the default **Administrator** role.

To edit the permissions for a user role

1 Go to **User > User Roles**.

2 In the **User Roles** list, select the role of interest and click **Edit Role**.

3 Edit the **Description** field of the **Add Role** dialog box and edit permissions for the role.

4 Click **Save**.

Delete a User Role

You can delete a user role from the Polycom CMA system, provided no users are currently assigned to it.

To delete a user role

1 Go to **User > User Roles**.

2 In the **User Roles** list, select the role of interest and click **Delete Role**.

3 Click **Yes** to confirm the deletion.

The user role is deleted from the Polycom CMA system.

18

System Reports

This chapter describes how to view and export reports available for the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Site Statistics Report

Use the **Site Statistics** report to check call rate and call quality statistics for the sites. You can view the data in a grid or graphically.

To view Site Statistics

1. Go to **Reports > Site Statistics**.

   The **Site Statistics** list appears with the data displayed in a grid.

2. To view the **Site Statistics** graphically:

   a. Click **View Chart**.

   b. In the **Site Name** list, select the site(s) to chart.

   c. In the **Y-Axis** list, select the statistic(s) to chart.

   d. In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

      The charts are dynamically updated with your choices.

Site Link Statistics Report

Use the **Site Link Statistics** report to check call rate and call quality statistics for all site links. You can view the data in a grid or graphically.

To view Site Link Statistics

1. Go to **Reports > Site Link Statistics**.

   The **Site Link Statistics** list appears with the data displayed in a grid.

2. To view the **Site Link Statistics** graphically:

   a. Click **View Chart**.

   b. In the **Site Name** list, select the site(s) to chart.

   c. In the **Y-Axis** list, select the statistic(s) to chart.

   d. In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

      The charts are dynamically updated with your choices.

Call Detail Record Reports

Two report pages provide call detail record (CDR) information: **CDR Table: IP View** and **CDR Table: ISDN View**.

To work with the Call Detail Records, extract them from the appropriate database table. For IP Call Detail Records, extract `Logger.dbo.calls`. For ISDN Call Detail Records, extract `Logger.dbo.DM_CDRLog`. See your Microsoft SQL Server documentation for information about extracting data.

You can use data from the reports to troubleshoot problems, provide information about network traffic, and ensure accurate billing for video calls.

Note

To be included in the ISDN CDR, endpoints in the call do not need to be currently registered with the gatekeeper or global directory server. To be included in the IP CDR, endpoints must be registered through the gatekeeper.

IP Call Detail Records

Note
IP calls through the Global Address Book that are not registered to the gatekeeper do not display in this report.

To view the IP Call Detail Records report

1 Go to **Reports > IP Call Detail Records**.

The **IP Call Detail Records** report appears. It lists the 5,000 most recent IP calls made to or from system-managed devices for the current date. It includes the following information.

Column	Description
Call ID	ID automatically generated for the call.
Conf ID	The GUID (global unique identifier) for the conference.
Date/Time	Date and time the call started, provided in local time for the server.
Source	Name, IP, or alias of the device that originated the call.
Source Address	IP address of the device that originated the call.
Destination	Name, IP address, or alias of the device that received the call.
Destination Address	IP address of the device that received the call.
Call Type	The type of call: scheduled or unscheduled.
Bandwidth (Kbps)	Bandwidth that was used for the call.
Duration (min)	Length of the call in minutes, up to a maximum of 999.
Q.850 Code	Standard cause code for call termination.

2 Use the **Filter** to customize the report by **Date**, **IP Address**, **Device Type**, **Call Type** and **Duration**.

ISDN Call Detail Records

To view the ISDN Call Detail Records report

1 Go to **Reports > ISDN Call Detail Records**.

The **ISDN Call Detail Records** report appears. It lists the 5,000 most recent IP calls made to or from system-managed devices for the current date. It includes the following information.

Column	Description
Call ID	ID automatically generated for the call.
Conf ID	The alphanumeric value that identifies the conference. **Note** This value is only available for multipoint conferences.
Date/Time	Date and time the call started, provided in local time for the server.
System Name	Name, IP, or alias of the device that originated the call.
Remote Site	Name, IP, or alias of the device that received the call.
Direction	Indicates whether the call was inbound or outbound.
Call Type	The type of call: scheduled or unscheduled.
Bandwidth (Kbps)	Bandwidth that was used for the call.
Duration (min)	Length of call in minutes, up to a maximum of 999.
Cause Code	Standard Q.850 cause code for call termination.

2 Use the **Filter** to customize the report by **Date**, **IP Address**, **Device Type**, **Call Type** and **Duration**.

Endpoint Usage Report

Note
The Endpoint Usage Report is for registered Polycom HDX system endpoints only.

To view the Endpoint Usage Report

1 Go to **Reports > Endpoint Usage Report**.

A list of the registered Polycom HDX system endpoints appears.

2 Select one or more endpoints to include in the report and click **Generate Report** that appears.

The **Summary** usage report for the selected endpoints appears. It includes the following information.

Field	Description
Start Date	The start date for the report. This defaults to the current date.
End Date	The end date for the report. This also defaults to the current date.
Number of calls	The number of calls the selected endpoints joined for the selected date range. Click **Details** to get the following information about these calls: • **Call ID**—A system-generated call identifier • **Connection Type**— • Start Time • End Time • Call Type • Bandwidth • From • To
Total call time	The total amount of time the selected endpoints spent in calls during the selected date range.
Average time per call	The average duration of calls the selected endpoints joined during the selected date range.
Scheduled calls	The number (and percentage) of calls the selected endpoints joined during the selected date range that were scheduled using one of the Polycom CMA system scheduling interfaces.
Adhoc calls	The number (and percentage) of calls that the selected endpoints joined during the selected date range that were unscheduled.

The **Summary** usage report also charts the number of **Calls** versus the **Call Bit Rate (kbps)**.

Conference Summary Report

Use the **Conference Summary Report** option to review monthly summary information about past Polycom CMA system conferences.

To create a Conference Summary Report

1 Go to **Reports > Conference Summary Report**.

An empty **Conference Summary Report** grid appears.

2 As needed, change the **From:** and **To:** dates to select the date range for the report, and click **View**.

The **Conference Summary Report** for the selected date range appears. It includes the following information.

Column	Description
Date	Information is displayed on a month-by-month basis and an average for the selected months
Scheduled Confs	The number of conferences scheduled via one of the Polycom CMA system scheduling interfaces (that is, the Polycom CMA system application, the Polycom Scheduling Plugin for Microsoft Outlook, or the Polycom Scheduling Plugin for IBM Lotus Notes)
Adhoc Confs	The number of conferences that used one or more devices for which the Polycom CMA system was the gatekeeper, but that weren't scheduled via one of the Polycom CMA system scheduling interfaces
MP Confs	The number of multipoint conferences scheduled using one of the Polycom CMA system scheduling interfaces
P2P Confs	The number of point-to-point conferences scheduled using one of the Polycom CMA system scheduling interfaces
Gateway Confs	The number of scheduled conferences that used a gateway to reach one or more devices
Embedded MP Confs	The number of scheduled multipoint conferences that used the MCU embedded in a V-Series, VSX-Series, or Polycom HDX-Series device rather than an external MCU such as an MGC or RMX 2000

Column	Description
P2P Confs on MCU	The number of scheduled point-to-point conferences that used an external MCU such as an MGC or RMX 2000 even through point-to-point conferences do not usually require MCU resources
Short Confs	The number of scheduled conferences that were scheduled to last 30 minutes or more, but which actually lasted less than 30 minutes
Scheduled Minutes	The sum of the scheduled minutes for all Polycom CMA system scheduled conferences
Executed Minutes	The sum of the actual minutes for all Polycom CMA system scheduled conferences
Total Parts	The sum of the participants that joined Polycom CMA system scheduled conferences
Avg Parts in MP Confs	The average number of participants that joined scheduled Polycom CMA system multipoint conferences

3 To create one of the conference summary report charts, click the appropriate chart name below the grid. Chart choices include:

Column	Description
Scheduled vs. Adhoc	A chart that compares the number of scheduled conferences to the number of adhoc conferences for each month
Scheduled Types	A chart that compares the number of point-to-point, multipoint, gateway, and embedded multipoint conferences for each month
Scheduled vs. Executed Mins	A chart that compares the number of scheduled minutes to the number executed minutes for each month
Avg Parts in MP Confs	A chart that displays the average number of participants in multipoint conferences for each month
Point-to-Point Confs on MCUs	A chart that displays the number of point-to-point conferences hosted on an external MCU for each month

The selected chart dynamically appears below the grid.

4 To export the report:

a Click **Export**.

b In the **File Download** dialog box, click **Save**.

c In the **Save As** dialog box, browse to a location and click **Save**.

Gatekeeper Message Log

Use the **Gatekeeper Message Log** page to:

- View messages that endpoints send to the gatekeeper
- Define which messages are logged
- Pause and restart message logging
- Clear the log
- Export the log to another file

Logging starts when you define the **Log Settings**. Logging stops only when you clear all of the **Log Settings**. Logging can include these types of messages:

- **Warnings/Errors.** Messages displayed for all warnings or errors that occur on registered Polycom endpoints
- **Rogues.** Messages displayed for all calls from unregistered endpoints
- **Events.** Messages display about these events:
  - Registration
  - Call detail
  - Neighboring gatekeeper

While you can pause logging, the Polycom CMA system always logs device errors and warnings.

You can also:

- Clear events from the log, which removes data from the database
- Export the log to a a comma-separated value (CSV) file. You can export only the data that displays on-screen, and exporting the log may take a long time depending on the number of entries in the log.

View and Export the Gatekeeper Message Log

To see more details about a log message

1. Go to **Reports > Gatekeeper Message Log**.
2. Use the **Filter** on the **Gatekeeper Message Log** list to customize the list.
3. Select the message of interest.

   The **Gatekeeper Message Log** report appears. It has these fields:

Column	Description
Type	These types of messages display: • Information, which indicates normal communications between the Polycom CMA system and the endpoint. • Warning, which indicates an unscheduled call and the inability to assign E.164 and ISDN numbers to an endpoint. • Error, which indicates the registration of an endpoint or a call failed, or a lack of resources for this gateway or MCU exists.
Date/Time	Date and time of the event.
Category	Specifies whether an event is a registration, call, or neighboring gatekeeper request.
Description	Displays the message sent to or received from the endpoint, identified by the IP address.

4 To export a message:

a Select the log of interest and click **Export Log**.

b In the **Export Log** dialog box, click **Yes**.

A `GKexport file` appears in your default text editor.

c Save the file.

Define Log Settings

To define which messages should be logged

1 Go to **Reports > Gatekeeper Message Log**.

2 When the **Gatekeeper Message Log** page appears, click **Log Settings.**

3 In the **Gatekeeper Log Settings** dialog box, select the events to log and click **OK**.

The Polycom CMA system begins logging the types of messages you selected.

Clear Events from the Log

To clear all events from the log

1. Go to **Reports > Gatekeeper Message Log**.
2. When the **Gatekeeper Message Log** page appears, click **Clear Events.**
3. Click **Yes** to confirm the action.

   The **Gatekeeper Message Log** is cleared.

Pause and Restart Logging

To pause logging

1. Go to **Reports > Gatekeeper Message Log**.
2. When the **Gatekeeper Message Log** page appears, click **Pause Log.**
3. In the **Stop Logging** dialog box, click **Yes**.

   The **Start Log** button is available and the system stops logging device messages to the **Gatekeeper Message Log**.
4. Click **Start Log** to restart logging.

System Log Files

Many of the Polycom CMA system components can write a **System Log File** when they experience an error or issue. Whether or not they do write a system log file depends upon the system log level.

The following table lists some of the logs the Polycom CMA system saves.

Log Name	Description
Log Files Related to Basic System Functionality	
SE200MasterService.txt	Log file that shows when individual services are started and stopped, and displays a memory usage summary for some of those services (mqm, sitetopo, plcmgk, gab) every 30 minutes
SE200SerialConsoleLog.txt	Log file that shows when the serial console was started and which COM port was used (e.g. COM1). It also shows any errors that occur while processing menu commands from the serial console.

Log Name	Description
ESINSTALL-<*timestamp*>.txt	Log file that shows the output of the Polycom CMA system install script. shows what steps were done when installing the Polycom CMA system software
ESUPGRADE-<*timestamp*>.txt	Log file that shows the output of the Polycom CMA system upgrade script (not applicable unless an upgrade was performed)
Log File Related to Dial Plan Functionality	
DialRule_Log.txt	General log file used by the dial rule process. This process generates dial out strings to endpoints, controls the dialing rules set up in the user interface.
SiteTopo_Log.txt	When in debug mode, this log file contains messages about site topology entry and usage.
Log File Related to External Database Functionality	
ServiceMonitor_Log.txt	Log file for the redundancy service that shows when a redundant Polycom CMA system goes into active or standby mode
Log Files Related to Scheduling Functionality	
AdapterLog_SCH.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the scheduling component
Log Files Related to Global Address Book Functionality	
AdapterLog_GAB.txt	.NET remoting log file that shows low-level communication errors from the GAB communications with the integration layer
ComponentLog_GAB.txt	.NET remoting log file that shows low-level communication errors from the GAB communications with devices
EXXX_LOG*x*.txt	Log files for web services, device manager, and conference monitoring.
Log Files Related to Device Management Functionality	
AdapterLog_GMS.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the management component
<*DeviceType*>Device.txt	Log file that captures device specific message

Log Name	Description
*<DeviceType>*DeviceCollection.txt	Log file that captures device specific message
*<DeviceType>*PasswdErrs.log	Log file that captures device specfic messages related to potential password mismatchs
DeviceManager.txt	Log file for the device management process
DeviceManagerService.txt	Log file for the device management process
SoftUpdate	Log file that shows when a device is updated with a new software package via a scheduled softupdate
Log Files Related to Gatekeeper Functionality	
AdapterLog_PN.txt	.NET remoting log file that shows low-level communication errors between internal system components--in this case, the gatekeeper component
PN_Log.txt	General gatekeeper log file
MQM_Log.txt	General media quality monitor log file that will show any errors when writing CDRs or media quality data to the database
Log Files Related to Call Management Functionality	
Messages.txt	Conference launching log used exclusively by CodecMngr process. This log contains information about the conference start up process, i.e., information that the system sends to devices at the start of a conference.
CS_<*conf_name*>.html CS_<*conf_name*>.txt	Conference scheduling log used by the conference scheduling process. This log contains debug information on how a conference is created. A log file is created for each scheduled conference, with the log file name format: CS-<*conf_name*>.txt, where <*conf_name*> is the name of the scheduled conference. This is always on, and there is no logging level.
Log Files Related to Web Services Functionality	
apache_access.log.<*xxxx*>	Apache web server access log that shows when and what url was requested
apache_error.log	Log file that captures error messages from the Apache web server

Log Name	Description
mod_jk.log	Log file that shows which web requests were forwarded from Apache web server to the Tomcat servlet engine.
Log Files Related to Presence Functionality	
Jserver.log.*<n>*	Log file that shows errors related to the internal LDAP server and provisioning functionality. This circular log has a six month limit. The timestamp is the local server time.
boot.log	JBoss startup log. JBoss is the container service for the Jserver service
debug.log	Openfire debug log that shows errors related to connection to internal LDAP server.
error.log	Openfire error log
info.log	Openfire information log
warn.log	Openfire warning log
openfire.log	Openfire service log that shows when Openfire was started and problems related to its startup

View and Export System Log Files

To view System Log Files

1 Go to **Reports > System Logs**.

The **System Log Files** list appears listing the logs for the given time period.

2 To view a log file:

a Select the log file of interest.

b Click **Open**.

3 To export a `.zip` of all log files:

a Click **Get All**.

b To open the `.zip` file, in the **Open File** dialog box, click **Open with**, and browse to the program you use to open .`zip` files.

c To save the `.zip` file to your local computer, in the **Open File** dialog box, click **Save**.

4 Click **OK**.

Change the System Log Level

To edit the current system log level

1 Go to **Reports > System Logs**.

The **System Log Files** list appears listing the logs for the given time period. The **Current Log Level** indicates which log files are being saved.

2 Change the log level, by selecting a new value in the **Current Log Level** menu. Choices include:

- Debug
- Info
- Warn
- Error
- Major
- Fatal
- Off

3 In a redundant configuration, repeat steps 1 and 2 on the redundant server.

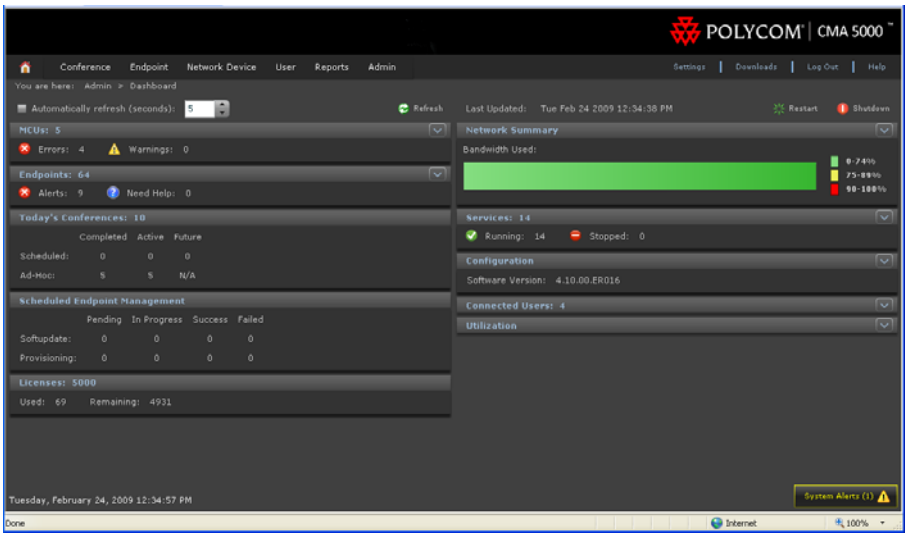
19

System Administration Overview

This chapter describes the Polycom® Converged Management Application™ (CMA™) system **Dashboard**, menu, and commands. It includes these topics:

Polycom CMA System Dashboard

When you log into the Polycom CMA system with **Administrator** role and permissions, the system **Dashboard** appears. Use the system **Dashboard** to view information about system health and activity levels.



The **Dashboard** has these sections:

Section	Description
Automatic Refresh	By default, the system **Dashboard** refreshes every 5 seconds. You can change this to a value of 5 through 60. The **Last Updated** field flashes when the system refreshes the **Dashboard** or when you click **Refresh**. If for some reason the system is unable to populate a section of the **Dashboard** data, the border around the section is highlighted in a blurry red. In this case, the data in that section may not be accurate. Note that all **Dashboard** information may become stale between automatic refreshes. The next refresh brings the information up-to-date
MCUs	Displays information about the Polycom MCUs (MGC or RMX) registered to the Polycom CMA system. The summary view displays the number of MCUs registered and the number of MCUs experiencing errors or warnings. The detailed view identifies the MCUs by **Name**, **Type**, **IP Address**, and **Status**.
Endpoints	Displays information about the current health and status of the endpoints registered to the Polycom CMA system. The summary view displays the number of endpoints registered to the Polycom CMA system and the number of endpoints experiencing alerts or requesting help. The detailed view displays graphically the number of endpoints that are **In Call**, **Online**, and **Offline**. The detailed view also displays a list of devices requiring attention by the device **Status**, **Name**, **Type**, and **IP Address**. Hover over the device **Status** to learn more about the device state.
Today's Conferences	Displays information about the number and status of scheduled and unscheduled (**Ad hoc**) conferences for the current day (as determined by the client system's time) including **Completed**, **Active**, and **Future** conferences.
Scheduled Endpoint Management	Displays information about the number and status of **Scheduled Provisioning** events and **Scheduled Softupdate** events. Valid states include: **Pending**, **In Progress**, **Success** or **Failed**.
Licenses	Displays information about the totall number of Polycom CMA system seats licensed to the system, and the number that are used and unused.

Section	Description
Network Summary	Displays information about network usage. The summary view displays the percentage of bandwidth currently in use by site. The detailed view lists the site links and their network performance information including **Name**, **Bandwidth**, **Calls**, **Delay**, **Jitter**, and **Packet Loss**. You can enable Real-Time Statistics for the network summary via the Primary Gatekeeper settings. See "Edit the Primary Gatekeeper Settings" on page 271.
Services	Displays information about the Polycom CMA system service processes. The summary view displays the number of **Running** and **Stopped** services. The detailed view displays a list of the service processes by **Service Name** and **Status**. See "System Services" on page 205.
Configuration	Displays information about the configuration of the Polycom CMA system. The summary view displays the current software version. The detailed view displays the amount of **Physical Memory** installed, whether or not the system is configured to use an **LDAP** directory, whether the **Database** the system uses is internal or external, whether the **Time Source** is internal or external, and whether or not the system is configured for **Redundancy**. The **Redundancy** field may also show two configuration errors: **Need Virtual IP** or **Secondary Is Down**.
Connected Users	Displays information about all users currently connected to the Polycom CMA system. The summary view displays the total number of connected users. The detailed view provides a breakdown of the number of users according to the standard Polycom CMA system user roles and permissions (**Administrator**, **Operator**, and **Scheduler)**. It lists users by **Username**, **Role**, and **Login Timestamp**.
Utilization	Displays information about system usage. The detailed view graphically displays the percentage of **CPU** and **Paging File** usage.

Dashboard Commands

Four commands are available from the **Dashboard** view. They are:

Command	Use this command to....
Refresh	Update the page with current status
Restart 	Shuts down and restarts the Polycom CMA system. See "Restart or Orderly Shut Down a Polycom CMA System" on page 336.
Shutdown 	Shuts down the Polycom CMA system. See "Restart or Orderly Shut Down a Polycom CMA System" on page 336.

System Administration Menu

The system **Admin** menu gives users with administrative permissions access to the day-to-day management tasks they need to monitor, maintain, and troubleshoot the Polycom CMA system. Besides the **Dashboard**, it lists these selections:

Selection	Use this selection to...
Conference Templates	Manage (add, edit, and delete) conference templates. See "Conference Templates" on page 207
Conference Settings	Enable or disable Conference Auto-launch and Conference Time Warning. See "Conference Settings" on page 214.
Provisioning Profiles	Manage (add, edit, and delete) automatic or scheduled provisioning profiles
Software Updates	Manage (add, edit, and delete) automatic or scheduled software update packages
Rooms	Manage (add, edit, and delete) rooms in the Polycom CMA system directory
Global Address Book	Manage (add, edit, and delete) users in the the Polycom CMA system Global Address Book
Server Settings	Configure the basic Polycom CMA system, which includes the network, system time, database, directory, licensing, redundancy, branding, GAB, remote alert, and email set up

Selection	Use this selection to...
Gatekeeper Settings	By default the Polycom CMA system is made the primary gatekeeper during the **First Time Setup** process. Use the **Gatekeeper Settings** option to modify the primary gatekeeper behavior or to add an alternate gatekeeper or neighboring gatekeepers. **Gatekeeper Settings** affect how devices register and calls are made in your video communications network. These settings allow you to: • Identify the gatekeeper with an identifier and description. • Specify registration-related settings, including the default gatekeeper, which endpoints register, the registration timeout period, and the offline timeout. • Set the maximum number of neighboring gatekeeper hop counts. • Specify how to handle calls to and from unregistered endpoints.
Management and Security	Upgrade the Polycom CMA system and configure the certificate, security, and endpoint management set up
Dial Plan and Sites	Edit the default Polycom CMA system **Dial Plan and Site** settings (which includes the definition of sites, site links, dial rules, services, and least-cost routing tables) to support your network topology and video call routing.
Alert Settings	Configure the Polycom CMA system to send email alerts for specified system or endpoint events
Database Backup FIles	View or backup the Polycom CMA system internal database backup file

System Services

The Polycom CMA system dashboard displays information about its service processes.

When users log into a Polycom CMA system, the system first checks to make sure all essential services are running before allowing users access to the system.

The following situations may occur.

- If all essential services are running, users are allowed to access the system.
- If one or more essential services is down, and the Apache service has been running for less than seven minutes, users receive an error message saying, “The Polycom CMA system is not ready. Please try again in a few minutes.”

- If one or more essential services is down, but the Apache service has been running for at least seven minutes, users are allowed to access to the system. In this case, specific system functions may be unavailable to users.

The following table lists the Polycom CMA system services and whether or not they are considered essential.

Service	Purpose	Comment
Apache	Web service	Essential
MSSQLSERVER	Database service	Essential
Openfire	Presence service	Required for presence
Polycom Cascader	Cascaded conferencing service	Required for cascading conferences
Polycom Conference Scheduling Service	Conferencing service	Essential
Polycom Device Manager	Device Manager service	Essential
Polycom DialRuleService	Dial rule service	Essential
Polycom Gatekeeper	Gatekeeper service	Essential
Polycom JServer	Java application service	Essential
Polycom Master Service	Service management service	Essential
Polycom Serial COM	Serial port service	Essential
Polycom Service Monitor	Redundancy monitoring service	Required for redundancy
Polycom SiteTopoService	Site topology service	Essential
Polycom Global Address Book	Global Address Book service	Essential

20

Conference Setup Overview

This chapter includes information about conference templates, options, and settings within the Polycom® Converged Management Application™ (CMA™) system. Two types of configuration settings relate to scheduled conferences:

- Conference Templates define most of the settings that become the defaults for a conference.
- Conference Settings are global system-wide settings that apply to all scheduled conferences.

Conference Templates

Conference templates allow you to create various combinations of settings to apply to scheduled conferences.

- For scheduled conferences that land on MGC devices, the conference template explicitly identifies the settings the MGC should use to control the conference.
- For scheduled conferences that land on RMX devices, the conference template explicitly identifies the RMX profile which identifies the settings the RMX should use to control the conference.

Administrators with **Conference Setup** permissions can add or edit **Conference Templates**. They can also identify (by user role) which users have access to which **Conference Templates** and which users have **Advanced** scheduling permissions. Then users select from the different templates available to them to switch between different combinations of conference settings.

Table 20-1 *Conference Template Parameters*

Field	Description
General Info	
Name	A meaningful name for the template, which can be up to 32 characters long
Description	A description (ASCII only[a]) of the conference settings template
Template Avail For	The roles to which users must be assigned to select this template when scheduling conferences
Video Settings	
Video Dial Options	These settings apply only to video conferences. The video dial options are: • Dial-In Only (all participants dial in to the conference) • Dial-Out Only (all participants are called) • Dial-In + Dial-Out (The person setting up the conference can specify which individual resources dial in or dial out.)
Video Mode	Sets the video layout for the conference. The default is video switching mode. To change to a Continuous Presence layout or mode, click the switching icon. The video mode determines the initial layout on an endpoint's display during a multipoint conference. This option requires an MCU. **Note** Make sure you have defined video endpoint systems and boards so that they are available for selection in continuous presence layouts.

Table 20-1 *Conference Template Parameters*

Field	Description
Video Algorithm	Sets the compression algorithm that the MCU uses to process video. Possible values include: • **Auto** • **H.261**. An ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • **H.263**. Based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • **H.264** The default is **Auto**. **Notes** • Selecting a video algorithm doesn't guarantee that it will be chosen for a conference since the MCU device may negotiate a different algorithm with the endpoints, depending on the endpoint's capabilities. • Not user-configurable for RMX devices
People and Content	Enable this setting when you have equipment that supports the display of people and content. Sets the format type of the content. Possible values include: • **None** • **People+Content** • **People and Content V0**. To show both the presenter and the content on a single display using HDX-Series products. • **Polycom Visual Concert PC**. To show live PC content using standard ViewStation® systems • **Polycom Visual Concert FX**. To integrate a laptop with graphics into a video call using ViewStation® products • **DuoVideo** **None** is the default. **Notes** • The MGC requires that conferences with **People and Content** use a minimum speed of 192 K. • Not supported on RMX devices. H.239 multimedia is set in the RMX profile for RMX devices.

Table 20-1 *Conference Template Parameters*

Field	Description
Lecture Mode	Possible values include: • **None**. All participants see the conference in the video mode defined elsewhere. • **Presentation Mode**. In this mode, when a participant's speech exceeds a predefined time (30 seconds), the system identifies the participant as the lecturer. The video mode for the other participant's automatically changes to full screen, displaying the lecturer, while the lecturer's endpoint displays participants in the video mode defined previously. When another participant starts talking, **Presentation Mode** is cancelled and the conference returns to its predefined video layout. **Notes** • Set in the RMX profile for RMX devices • RMX 1000 systems do not support **Lecture Mode**, **Presentation Mode**, or **Lecture View Switching**.
Speed	Sets the speed for the conference, which applies to both point-to-point and multipoint calls. Possible values are between 128 to 4096 Kbps and **Bridged Audio**. The default is 384 Kbps. **Notes** • This setting does not apply to **Audio Only** conferences. • For conferences that may land on an RMX device, the speed designated here is used to reserve bandwidth and must match the line rate defined in the RMX profile that is identified in the **Profile Name** field.
Lecture View Switching	Enables automatic switching of participants on the Lecturer's screen when **Lecture Mode** is set to **Presentation Mode** and the number of participants exceeds the number of windows identified by the video mode defined elsewhere. **Note** RMX 1000 systems do not support **Lecture Mode**, **Presentation Mode**, or **Lecture View Switching**.
High Definition	Select for an ultra-high quality video resolution enabling compliant endpoints to connect to conferences at resolutions of 1280x720 (720p) and at bit rates up to 4Mb.
Video Quality	Optimizes the video quality based on the amount of movement contained in the conference video. Possible values include: • **Motion**. Provides a higher frame rate without increased resolution • **Sharpness**. Provides a higher video resolution and requires more system resources

Table 20-1 *Conference Template Parameters*

Field	Description
MCU Settings	
Supported MCUs	Specify the supported MCU types. Possible values include: • MGC • RMX
RMX Profile Name	Identifies the RMX profile for the conference, if the conference ends up on an RMX device. **Note** Conferences fail if they land on an RMX device and a valid RMX profile is not specified.
Always Use MCU	When selected, an MCU is used for the scheduled conference, regardless of the number of participants. When not selected, an MCU is used only when necessary.
Conf Settings	
Meet Me Per Conference	When selected, only one dial-in number is assigned to the conference. When cleared, each dial-in participant is assigned a different dial-in number. **Note** Not supported on RMX devices.
Conference on Port	When selected, this option conserves bandwidth and ports by putting all participants on a single port. When Conference on Port is enabled, the Video Mode must be set to one of the Continuous Presence layouts. **Note** Not supported on RMX devices.
Conference Requires Chairperson	Select this option to enable an endpoint to control the conference. When this option is implemented, the conference scheduler can specify a four-digit number that the conference chair must use to control the conference. H.243 chair control allows an endpoint to control the conference using the H.243 chair control feature. The chairperson can disconnect participants, force the use of a continuous presence video layout, and terminate the conference. H.243 cascade control allows the MGC-50 or MGC-100 to support a cascading configuration of conferences with the capabilities of H.243. **Note** • Set in the RMX profile for RMX 2000 devices • The RMX 1000 system does not support the **Chairperson** feature.

Table 20-1 *Conference Template Parameters*

Field	Description
Entry Tone	Sets an entry tone sound when a participant enters a conference. **Note** Not user-configurable for RMX devices
Exit Tone	Sets an exit tone sound when a participant leaves a conference. **Note** Not user-configurable for RMX devices
End Time Alert Tone	Sets an alert tone to sound near the end of the conference. **Note** Not user-configurable for RMX devices
Talk Hold Time (sec)	Indicates the minimum period that a participant has to speak to become the main speaker. During this period, no other participant may become the main speaker. The range is from 1.5 seconds to 10 seconds, in increments of 0.01 seconds. **Note** Not user-configurable for RMX devices
End Time Alert (minutes)	Specifies the number of minutes before the conference end that the **End Time Alert Tone** should sound. **Note** Not user-configurable for RMX devices

Table 20-1 *Conference Template Parameters*

Field	Description
T120 Rate	Determines whether T.120 is enabled, and if so, the default transfer rate. Enable this setting when you have equipment that supports T.120 display of data. Options are: 6.4, 14.4, 16, 22.4, 24, 30.4, 32, 38.4, 40, 46.4, 54.4, and 62.4. **Notes** • Because this setting uses resources on the MCU device, it is recommended that you select **None**. • Not supported on RMX devices.
Audio Algorithm	Sets the compression algorithm that the MGC uses to process audio. The default is **Auto**. **Notes** • Selecting a certain video/audio algorithm doesn't guarantee that it will be chosen for a conference since an MGC device may negotiate a different algorithm with the endpoints, depending on the endpoint's capabilities. • Not user-configurable for RMX devices
Audio Mix Depth (sites)	Sets the number of participants with the loudest voices who can speak at once during a conference. If additional participants speak, their comments are not heard. **Note** Not user-configurable for RMX devices

a. For more information, see "Field Input Requirements" on page 6.

Polycom CMA system has a **Default Template**. Administrators with **Conference Setup** permissions can edit the **Default Template** and create additional templates with different settings.

When scheduling a conference, the **Default Template**, which is available to all users, is selected by default. Schedulers can select a different conference template from the list of templates an administrator has made available to them. Users with advanced scheduling permissions can edit the template settings for a specific scheduled conference. These changes apply only to the specified conference.

Use these best practices when working with conference templates.

- For the **Default Template**, select settings that are the lowest common values for all device types. This ensures that all conferences scheduled with the **Default Template** can successfully launch on whatever devices the system has available at the time.

- When creating new templates, give them meaningful purposes and names so that your users can easily identify the differences between template choices. For example, identify templates according to maximum bit rate, specific features implemented by the template (for example, Lecture Mode or Chairperson Control), and/or supported MCU type (MGC or RMX).
- In a mixed-MCU environment, consider the advantages and disadvantages of creating one or more conference templates for each MCU type. This ensures that the system can select a specific type of MCU and can implement the chosen conference settings.
- Remember that the RMX profile may override settings specified when scheduling a conference through the Polycom CMA system. To ensure consistent and expected behavior, make sure to synchronize and lock down RMX profiles and Polycom CMA system conference templates.

Note
Polycom CMA systems do not support scheduling of third-party MCUs. Template settings apply only to the MGC or RMX devices.

Conference Settings

Conference settings apply to all conferences scheduled using the Polycom CMA system. These settings include:

Field	Description
Conference Auto Launch	When **Disable** is selected, scheduled conferences do not start. This is useful if you wish to stop future scheduled conferences from starting before you perform a restart or shutdown.
Conference Time Warning	Specifies whether or not a message is sent to video endpoint systems to let users know that the conference is ending soon. The video endpoint system must support this feature. By default, **Conference Time Warning** is enabled.

21

Conference Setup Operations

This chapter includes information about conference options and tasks within the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

View the Conference Templates List

To view the Conference Template list

>> Go to **Admin > Conference Templates**.

The **Conference Templates** list appears.

Add a Conference Template

To add a conference template

1. Go to **Admin > Conference Templates**.
2. On the **Conference Templates** list, click **Add**  .
3. Complete the **General Info**, **Video Settings, MCU Settings,** and **Conf Settings** sections of the **Add Conference Template** dialog box.

4 Click **OK**.

The new template appears in the **Conference Template** list.

Note

The Polycom CMA system does not validate the **Conference Template** settings. When you create a new conference template, you must make certain that the settings match the capabilities of the MCUs (MGC or RMX device) or endpoints.

Edit a Conference Template

To edit a conference template

1 Go to **Admin > Conference Templates**.

2 On the **Conference Templates** list, select the template of interest and click **Edit**  .

3 Edit the **General Info**, **Video Settings, MCU Settings,** and **Conf Settings** sections of the **Edit Conference Template** dialog box as required.

4 Click **OK**.

Delete a Conference Template

To delete a conference template

1 In the **Conference Setup** menu, choose **Conference Templates**.

2 On the **Conference Templates** list, select the template of interest and click **Delete**  .

3 Click **Yes** to confirm the deletion.

Set Conference Settings

To specify conference settings

1. Go to **Admin > Conference Settings**.
2. On the **Conference Settings** page, make the required selections. "Conference Settings" on page 214.
3. Click **Update**.

Disable Conference Auto-Launch

To disable conference auto-launch

1. Go to **Admin > Conference Settings**.
2. In the **Conference Auto-Launch** section of the **Conference Settings** page appears, check the **Disabled** checkbox.
3. Click **Update**.

Disable Conference Time Warning

To disable the conference time warning

1. Go to **Admin > Conference Settings**.
2. In the **Conference Auto Launch** section of the **Conference Settings** page appears, uncheck the **Enabled** checkbox.
3. Click **Update**.

22

Room Overview and Operations

This chapter describes how to set up rooms in the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Local and Enterprise Meeting Rooms

The Polycom CMA system allows an administrator with **System Setup** permissions to manage local and enterprise meeting rooms and the devices associated with those meeting rooms.

Most often a Polycom CMA system is integrated with an enterprise directory from which rooms can be added. However, the Polycom CMA system also allows an administrator with **System Setup** permissions to add local rooms (i.e., users added manually to the system) and associate them with devices.

View the Rooms List

To view the Rooms list

>> Go to **Admin > Rooms**.

The **Rooms** list appears. It can be filtered by **Site**.

Column	Description
Resource Name	The unique and required name of the room
Description	The optional description of the room
Associated Devices	The primary device associated with this room. A set of elipses (...) indicates the room has more than one associated device.

Add a Local Room

When you add a local room (a room not found in the enterprise directory) to the Polycom CMA system, you specify settings for it and associate one or more devices with it.

To add a local room

1. Go to **Admin > Rooms**.
2. On the **Rooms** page, click **Add**  .

   The **Add New Room** dialog box appears.
3. If you are logged into a domain other than the Local domain, the click **Manually Define**.
4. Complete the **General Info** and **Associated Devices** sections of the **Add New Room** dialog box. The following table shows the room information in the Polycom CMA system records.

Field	Description
General Info	
Room Name	The name of the room, which appears in the address book for associated devices
Description	(Optional) A useful description (ASCII only[a]) of the room
Site	(Optional) The site in which the room is located **Note** Rooms and the endpoint associated with them must be assigned to the same site.
Email	(Optional) The email address of the room administrator
User ID	A unique user ID for the room. This user ID must be unique across all rooms and users and across all domains.

Field	Description
Password/ Confirm Password	
Associated Endpoints	
Available Endpoints	The list of unassigned endpoints that are managed by the Polycom CMA system
Selected Endpoints	The list of endpoints assigned to the room. The device at the top of the list is the primary device. You can change the order of device priority by selecting a device and clicking **Move Up** or **Move Down**.

a. For more information, see "Field Input Requirements" on page 6.

5 Click **OK**.

The new room appears in the list.

Add an Enterprise Room

If your Polycom CMA system is integrated with an enterprise directory, you can add a room in the enterprise directory to the Polycom CMA system.

To add an enterprise room

1 Go to **Admin > Rooms**.

2 On the **Rooms** list, click **Add Room**  .

The **Add New Room** dialog box appears. The **Find Room in LDAP** page with a search field is displayed.

3 To find a room in the enterprise directory:

- **a** Select the required LDAP **Domain**.
- **b** Select a **Search Attribute** on which to search the enterprise directory and enter a **Search Value**. For information on searching see "Filter and Search a List" on page 7.
- **c** Click **Search**.

  A list of the enterprise users that meet the search criteria appears. If the search found more than 500 matching entries, only the first 500 are displayed.
- **d** Select the room of interest and click **Define Details**.

4 To add a room manually, click **Manually Define**.

5 Complete the **General Info** and **Associated Devices** sections of the **Add New Room** dialog box.

> **Note**
> User IDs must be unique across all users and rooms and across all domains.

6 Click **OK**.

The room is added to the Polycom CMA system.

Edit a Room

To edit a room

1 Go to **Admin > Rooms**.

2 In the **Rooms** list, select the room of interest and click **Edit**  .

3 As required, edit the **General Info** and **Associated Devices** sections of the **Edit Room** dialog box.

> **Note**
> User IDs must be unique across all users and rooms and across all domains.

4 Click **OK**.

Delete a Room

To delete a room

1 Go to **Admin > Rooms**  .

2 In the **Rooms** list, select the room of interest and click **Delete**.

3 In the **Delete Room** dialog box, click **Yes**.

The room is deleted from the Polycom CMA system.

23

Directory Setup Operations

This chapter describes how to manage the Global Address Book in the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Global Address Book

The Polycom CMA system Global Address Book is a shared directory managed by the Polycom CMA system that allows users to look up and call other users (with devices) in their video communications network. The Global Address Book, which is an instance of a Global Directory Service, can also include contact information for endpoints outside the network, third-party endpoints, and other endpoints that cannot register with the gatekeeper, such as ISDN-only endpoints. An administrator must add these endpoints manually.

Manual entries are also called static entries, because they are not updated when information at the endpoint changes.

Note

When manually registering third-party endpoints, you may need to configure the endpoint with the (case-sensitive) path to the Polycom CMA system Global Address Book.

When an endpoint registers with the Polycom CMA system, its information is automatically entered into the Global Address Book. When information changes at the endpoint, the Global Address Book is automatically updated as well.

Only administrators can add, edit, or delete information in the Global Address Book. If an endpoint is configured to **Allow Directory Changes**, additions and deletions to the Global Address Book are pushed to the endpoint.

Note

- The Polycom CMA system Global Address Book lists devices. Devices may or may not have users (or rooms) associated with them. The Global Address Book cannot list users unless they have devices associated with them.
- If your company has more than 100 endpoints, don't limit the Global Address Book on the endpoint side or the user won't have access to all Global Address Book entries.

From a video endpoint system, end-users can locate other users' devices by name in the Global Address Book and initiate a call without knowledge of another user's equipment.

Note

Endpoints also have an address book. Users can add personal entries to their endpoint address book. These entries are not communicated to the Global Address Book.

View the Global Address Book

To view the Global Address Book

1. Go to **Admin > Global Address Book**.
2. As needed, use the **Filter** to customize the **Global Address Book**. It can be filtered by **Address Type** (**Static**, **Dynamic**, or **All**) or **Attribute** (**Device Name**, **IP Address**, or **All**).

   The user information found in the **Global Address Book** includes:

Column	Description
User/Resource	The associated user or resource ID
Device Name	The name of the associated device
Type	The type of endpoint
IP Address	The IP address of the endpoint

Column	Description
Phone Number	The phone number of the endpoint
Alias	The alias associated with this device

Add a User to the Global Address Book

To add a user to the Global Address Book

1 Go to **Admin > Global Address Book**.

2 In the **Global Address Book**, click **Add GAB User**  .

3 Complete the **IP Video(H.323)** and/or **ISDN Video (H.320)** sections of the **Add GAB User** dialog box.

Field	Description
Name	The name (ASCII only[a]) of the endpoint
Use IP Video (H.323)	
Use ISDN Video (H.320)	
IP Video (H.323)	
IP Address	The IP address of the video endpoint system
E.164 alias	The alias associated with this endpoint
Rate	The maximum speed at which this endpoint can be called
ISDN Video (H.320)	
Country Code	The country code to dial to reach the endpoint
City Code	The area or city code in which the endpoint is located
Number A	The ISDN number of the endpoint
Number B	If the endpoint has a 2x64 ISDN line configuration, enter the second ISDN number of this endpoint
Extension	The extension number of the unit with gateway + extension dialing
Rate	The maximum speed at which this unit can be called

a. For more information, see "Field Input Requirements" on page 6.

4 Click **OK**.

Edit a Global Address Book User

You must edit the **Global Address Book** when the address information (ISDN number or IP address) for a static user changes. You cannot edit the **Global Address Book** for a dynamic user; their information comes from the endpoint registration.

To edit a static address in the Global Address Book

1. Go to **Admin > Global Address Book**.
2. As needed, use the **Filter** to customize the **Global Address Book**. It can be filtered by **Address Type** (**Static**, **Dynamic**, or **All**) or **Attribute** (**Device Name**, **IP Address**, or **All**).
3. Select the user of interest and click **Edit GAB User**  .
4. In the **Edit GAB User** dialog box, make the required changes.
5. Click **OK**.

Delete a Global Address Book User

You can delete users from the **Global Address Book**. However, if the user's endpoint registered with the **Global Address Book** dynamically, the user continues to reappear in the **Global Address Book** until you clear the **Publish** option at the endpoint.

> **Note**
> The **Publish** option may have different names on different endpoints. For example, on a ViewStation device, it is called **Register this system when Powered On**.

To delete a user from the Global Address Book

1. Go to **System Management > Directory Setup > Global Address Book**.
2. As needed, use the **Filter** to customize the **Global Address Book**. It can be filtered by **Address Type** (**Static**, **Dynamic**, or **All**) or **Attribute** (**Device Name**, **IP Address**, or **All**).
3. Select the users of interest and click **Delete GAB User**.
4. Click **Yes** to confirm the deletion.

   The selected user(s) are deleted from the **Global Address Book**.

Edit the Global Address Book Password

You can edit the password that must be entered at the endpoint to allow it to access the **Global Address Book**.

To edit the password for the Global Address Book

1. Go to **Admin > Global Address Book**.
2. In the **Global Address Book**, click **Set GAB Password**  .
3. In the **Set Client Password** dialog box, enter the **Old Password** and the **New Password**. (Note that the password fields are ASCII only; for more information, see "Field Input Requirements" on page 6.)
4. Confirm the new password and click **Save**.

24

Polycom CMA System Setup Overview

This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) **System Setup** menu. It includes these topics:

Server Settings

Most of the selections in the **Server Settings** menu are entered during the Polycom CMA system First Time Setup process and do not change frequently. Use the **Server Settings** menu, when you do need to change them.

The **Server Settings** menu allows users with Administrator permissions to implement the Polycom CMA system configuration best suited for their corporate environment as identified in the solution design, site survey, and/or network design.

The **Server Settings** menu includes these items:

Selection	Description
Network	The basic network setting for the Polycom CMA system on your network.
Gatekeeper Settings	By default the Polycom CMA system is made the primary gatekeeper during the **First Time Setup** process. Use the **Gatekeeper Settings** option to modify the primary gatekeeper behavior or to add an alternate gatekeeper or neighboring gatekeepers. **Gatekeeper Settings** affect how devices register and calls are made in your video communications network. These settings allow you to: • Identify the gatekeeper with an identifier and description. • Specify registration-related settings, including the default gatekeeper, which endpoints register, the registration timeout period, and the offline timeout. • Set the maximum number of neighboring gatekeeper hop counts. • Specify how to handle calls to and from unregistered endpoints.
Management and Security Settings	**Management Settings** allow you to upgrade the Polycom CMA system software and enable auto discovery of endpoints. **Security Settings** allow you to implement HTTPS for the Polycom CMA system.
Dial Plan Settings	Edit the default Polycom CMA system **Dial Plan and Site** settings (which includes the definition of sites, site links, dial rules, services, and least-cost routing tables) to support your network topology and video call routing.

Polycom CMA System Licensing

The seat capacity for a Polycom CMA 5000 system scales from 500 to 5,000 devices. The entry-level Polycom CMA 5000 system has a baseline capacity of 500 client access licenses. Additional licensing is offered in 100, 500, and 1000 license pack sizes.

The seat capacity for a Polycom CMA 4000 system scales from 200 to 400 devices. The entry-level Polycom CMA 4000 system has a baseline capacity of 200 client access licenses. Additional device licensing is offered in 100 license pack size.

Your system comes with a Default Trial key that is valid for 60 days after activating your system. With your system order, you will receive one License Certificate. You must activate the License Certificate to receive an activation key, which you then enter in the Polycom CMA system. When you enter this activation key into the system, it overwrites the Default Trial key.

When applied to the system, an expansion license pack augments the device license count. For example, applying a 1000-device expansion license pack to a baseline Polycom CMA 5000 system will yield a total license count of 1500 concurrent licenses.

Where applicable, the number of concurrent calls supported by a Polycom CMA system is derived from the number of device licenses at a 3/10 ratio (calls/devices). For example, a system licensed for 5000 devices supports up to 1500 concurrent calls in routed mode and 3000 calls in direct mode.

Device licenses are consumed based on a 1:1 basis for any managed device (endpoints, MCU, GK, GW— including personal endpoints, IP blades, and more) that can be added to the system by any means, including the user interface, registration for management services, or registration for Global Address Book services.

Note

Device licenses are consumed by managed devices, not by users. You may add any number of local or enterprise users to the Polycom CMA system.

The Polycom CMA system has the following licensing packages:

- Base system license
- Base system license with Microsoft Outlook
- Base system license with IBM Lotus Notes
- Base system license with Microsoft Outlook and IBM Lotus Notes
- Redundant system licenses (primary and redundant licenses)
- Redundant system licenses with Microsoft Outlook
- Redundant system licenses with IBM Lotus Notes
- Redundant system licenses with Microsoft Outlook and IBM Lotus Notes

Licensing for the Polycom CMA Desktop client is included with the Polycom CMA system. When a Polycom CMA Desktop client is provisioned by the Polycom CMA system, it automatically consumes a license. That license is then reserved for that Polycom CMA Desktop client. However, you can configure the Polycom CMA system to automatically released a Polycom CMA Desktop client license after a set number of days of inactivity.

Licenses consumed by registered devices are never automatically released. To release a license from a registered device, an administrator must manually delete the device from the system.

Polycom CMA System Site Topology and Dial Plan Set Up

The site topology you create within the Polycom CMA system should reflect your network design.

When setting up the site topology for a Polycom CMA system envision three hierarchical levels (Region > Sites > Subnet) and the links between them.

Regions

A region is the total area within a network that is managed by a single Polycom CMA system (or two Polycom CMA systems in a redundant configuration). A region is equivalent to a gatekeeper zone in H.323 configurations.

When you first set up the Polycom CMA system, a default region (**My Region**) is automatically created. As an administrator, you may change the name of the default region and add sites to the region.

Sites

Sites represent the different local area networks (LANs) within the region that the Polycom CMA system manages. A site usually corresponds to a geographic location such as a branch office or a particular building in an extended campus.

When you first set up the Polycom CMA system, two default sites (**Internet/VPN** and **Primary Site**) are automatically created. The **Internet/VPN** site is created outside the default region.The **Primary Site** is created within the default region. The default **Internet/VPN** site cannot be edited.

The LANs provide high bandwidth for IP traffic and may include multiple gateways to connect the IP network to the PSTN network.

Subnets

A subnet, which consists of a subnet IP network address and a subnet mask definition. This definition corresponds to the actual subnet mask used within the network, but can be either smaller or larger, depending on requirements for video. For example, if a single site has eight Class C subnets numbered sequentially, you can list all eight subnets individually within the site or a single, larger subnet that encompasses all eight subnets.

Notes

- Do not use a class A subnet. Examples 172.0.0.0 and 255.0.0.0 will not be recognized or work. As a minimum, use a class B network mask (for example, 172.22.0.0 and 255.255.0.0).
- You can assign a subnet to only one site. The Polycom CMA system does not allow overlapping subnets.

The Polycom CMA system identifies where devices are by their IP address and the system's subnet mask. Devices that have an IP address within a defined subnet for the Polycom CMA system can be provisioned, updated, and monitored. Devices that have an IP address in an undefined subnet have limited access to system features.

Site Links

Site links define the connections that exist between sites and indicate how routing occurs on your network. A site link is usually a limited-bandwidth, wide-area network (WAN) or virtual private network (VPN) connection that links two physical locations. The Polycom CMA system uses site links to manage bandwidth within a site and across sites.

There are two types of site links:

- Direct links are connections between two sites through a leased line, frame relay, or an asynchronous transfer mode (ATM) network, or from a site to the Internet. In addition, direct links are used for secure connections over the Internet, such as VPN. For each direct link, you must define the maximum available bandwidth and bit rate for calls. Network settings can have a higher bandwidth and bit rate than Polycom CMA system settings.

  Note

  The bit rate can be set at the network level, the device level, and the conference level. If there is a discrepancy between these bit rate settings, the system implements the lowest bit rate setting. The only exception, is that the bit rate in the RMX profile takes precedence over the bit rate in the conference settings.

- Multisite links are connections that require routing through a series of sites and may include a secure Internet connection. The Polycom CMA system generates multisite links from the site links added to the system.

  Note

  The Polycom CMA system can only generate multi-site links for up to 60 sites.

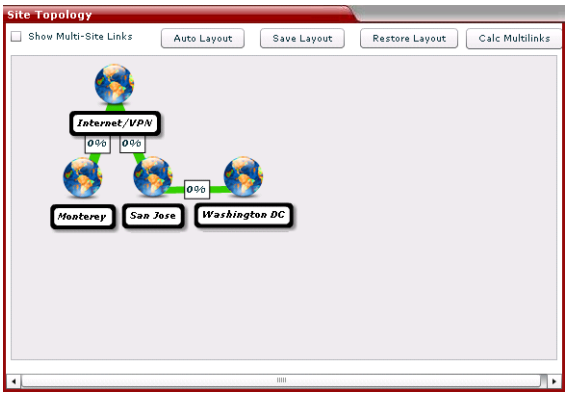
Site Topology and Site Link Examples

Two examples of site links follow: a simple, direct link and a complex, multisite link.

Figure 24-1 shows Company ABC, based in San Jose, CA. Company ABC has three sites in the United States: two in California (San Jose and Monterey) and one in Washington, D.C.

The San Jose site has a direct site link with a maximum bandwidth of 10 MB that connects it to the Washington, DC site. A second site link connects the San Jose site to the Monterey site. This link uses a virtual private network (VPN) connection so the connection between them is not direct, it is considered a multisite link. All three sites share the same the Polycom CMA system.

Figure 24-1 *Site Topology Example*

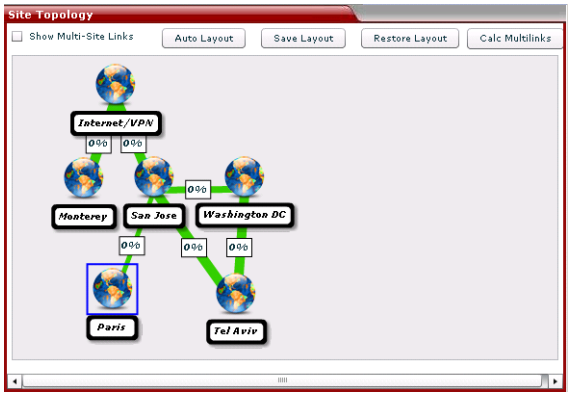


In the Polycom CMA system, define the site topology as:

- Three sites: Monterey, San Jose, and Washington
- Three direct site links, which include:
  - San Jose to Washington
  - San Jose to the Internet
  - Monterey to the Internet
- Two multisite links, which include
  - San Jose to Monterey (using links to the Internet)
  - Washington to Monterey (using links to the Internet)

Figure 24-2 shows the same Company ABC with two additional sites in Paris and Tel Aviv.

Figure 24-2 *Connecting Sites Through Multisite Links*



In the Polycom CMA system, define the site topology as:

- Five sites: Monterey, San Jose, Washington, Paris, and Tel Aviv
- Six direct site links, which include:
  - Monterey to Internet
  - San Jose to Internet
  - San Jose to Washington
  - San Jose to Paris
  - San Jose to Tel Aviv
  - Tel Aviv to Washington
- Seven multisite links, which include
  - Monterey to San Jose
  - Monterey to Paris
  - Monterey to Washington
  - Monterey to Tel Aviv
  - San Jose to Tel Aviv (via Washington)
  - Paris to Washington
  - Paris to Tel Aviv

Also note, there are two routes between San Jose and Tel Aviv. If one route is less expensive, you can enter least-cost routing information to make sure that route is used and maintain the other route as a backup.

Default Polycom CMA System Dial Plan Settings

The Polycom CMA system ships with a default dial plan configuration, which includes a region, site (but not a subnet within the site), dialing rules, and IP call routing. The default dial plan allows your video network to operate immediately. If necessary, you can modify the default dial plan to add functionality.

The default dial plan has these features and settings:

- The default gatekeeper region is called **My Region**. This default region includes the default site at which you have installed the Polycom CMA system. Gatekeeper region settings include the **Gatekeeper IP Address**, **Port**, and **Gatekeeper Identifier**.
- The default site is called **Primary Site**, which is the location at which you have installed the Polycom CMA system.
- All rogue calls are blocked by the gatekeeper when the Primary Gatekeeper setting **Deny calls to/from unregistered endpoints** is checked
- All MGC and/or gateway services registered with the gatekeeper are available to all endpoints

You can enable most features not available through the default dial plan by editing the default site. This includes these features:

- Automatic provisioning of E.164 aliases to IP H.323 endpoints
- Routing of inbound ISDN calls to correct endpoints
- Enabling outbound IP calls
- Allowing access through a firewall using an SBC device

You can add these features to your dial plan and video call routing setups:

- Routing H.323 calls to neighboring gatekeepers by adding new neighboring regions
- Adding gateway and MCU services manually if you have a third-party MCU that registers with the gatekeeper using a standard H.323 mechanism
- Adding bandwidth management capabilities by defining new sites and site links
- Adding IP to ISDN call routing using least-cost routing.

Site Settings

Field	Description
General Info	
Site Name	The physical location of the site. The name can be up to 32 characters long, and may include spaces, dashes, and underscores.
Description	Description (ASCII only[a]) of the site.
Override ITU Dialing Rules	Check this box to override the standard dialing rules established by the International Telecommunications Union.
PBX Access Code	The access code required to enter the site's PBX system.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
# of Digits in Subscriber Number	The number of digits in a phone number. For example, in the United States, subscriber numbers may have seven digits or ten digits depending upon the region.
Default LCR Table	The default least-cost routing table (LCR) for this site. This LCR table is used for all calls originating from devices associated with this site. The default is **None**.

Field	Description
Assignment Method	The ISDN number assignment method for the site. Possible values include: • **No Auto Assignment**. Select this option when ISDN numbers are not assigned to IP devices. • **DID (Direct Inward Dial)**. Select this option when you assign a range of phone numbers received from the telephone company service. • **Gateway Extension Dialing**. Select this option when you have a single gateway phone number and a range of extensions (E.164 aliases) that are internal to the company. In this case, calls go through a gateway. Endpoints are differentiated by the extension at the end of the dial string. When a site is assigned an automatic assignment method, devices without an ISDN number are assigned one when they register. These numbers allow inbound calls to reach specific video endpoints. After an ISDN number is assigned to an endpoint, it is reserved for use as long as that endpoint remains registered with the ReadiManager system. **Note** If you do not assign ISDN numbers automatically, you cannot call IP-only endpoints through an ISDN line.
ISDN Number Assignment—DID (Direct Inward Dial)	
# Digits in Call Line Identifier	Enter 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, 4 for internal calls, or 11 for callers in a different area code. • This number indicates what part of the full dial string is sent to the gatekeeper for address resolution.
# Digits in Short Phone Number	Enter 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. • This number indicates what part of the dial string is sent to the gatekeeper for address resolution in gateway + extension dialing.
ISDN Number Range - Start	The starting ISDN number to assign automatically to IP devices
ISDN Number Range - End	The ending ISDN number to assign automatically to IP devices

Field	Description
ISDN Number Assignment—Gateway Extension Dialing	
Gateway Phone Number	Phone number of the site gateway
E164 Start	• The starting number in a range of available extensions to assign automatically to IP devices • When a device without native ISDN registers, a number within the start and end range is assigned, so that the device can be called through an ISDN line
E164 End	The ending number in the range of available extensions to assign automatically to IP devices
Site Routing/Bandwidth	
Internet calls are not allowed	Disables call routing through the Internet
Allowed via H.323 aware firewall	Enables call routing through the Internet, using an H.323-aware firewall **Notes** • For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string. • If you select **Allowed via H.323 aware firewall** you must create a site link between this site and the Internet/VPN site.
Allowed via H.323 aware SBC or ALG	Enables call routing via the Internet, using an H.323-aware SBC (Session Border Control) or ALG (Application Level Gateway) server **Note** For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string.
Call Signaling Address	IP address of the SBC or ALG server. Supports only IPv4
Port	Port address of SBC or ALG server
Call Max Bit Rate (kbps)	
Site Subnet	
Subnet IP Address/Mask	

a. For more information, see "Field Input Requirements" on page 6.

Site Link Settings

Field	Description
Link Name	Name (ASCII only[a]) of the inter-site link
Description	Description (ASCII only[a]) of the inter-site link
From Site	Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.
To Site	Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet/VPN option.
Link Type	Specifies a direct link between two physical sites or a multisite link, for which a path of links is defined
Total Bandwidth (Kbps)	The maximum available bandwidth for audio and video, which you set at the gateway or router. Only applies to direct links. The bandwidth on multisite links is the lowest respective value from the list of direct links.
Call Max Bit Rate (Kbps)	The maximum bit rate allowed for an audio and video call. Only applies to direct links. The bit rate on multisite links is the lowest value in the list of direct links.

a. For more information, see "Field Input Requirements" on page 6.

Polycom CMA System LDAP Integration

All Polycom CMA system users work within an assigned domain—a set of users and devices on a network that are administered as a unit.

Domains are important in the Polycom CMA system because when users search for participants and rooms to add to a conference, they can only select from:

- Local users and rooms (i.e., users and rooms added directly to the Polycom CMA system)
- Users and rooms in their domain

To add participants or devices outside these domains, users must add them as guest participants.

Polycom CMA system administrators can add users in two ways. They can add users directly to the Polycom CMA system **Local** domain or they can integrate the system with an LDAP enterprise directory.

Note

The Polycom CMA system supports only the Microsoft Active Directory implementation of LDAP. LDAP is a client-server protocol that authenticates users automatically, which eliminates the need to re-enter IDs and passwords. LDAP also provides a uniform way to store and locate end-user information.

Enterprise directory integration provides these features:

- Access to user information
- Assignment of different roles to users in different enterprise groups
- Identification of enterprise resources, such as rooms, so that they can be treated as resources in the Polycom CMA system

A Polycom CMA system also supports child domains.

Polycom CMA System Gatekeeper Functionality

During the **First Time Setup** process, the Polycom CMA system is designated as the primary gatekeeper and the default gatekeeper settings are implemented.

The Polycom CMA system is the primary gatekeeper responsible for:

- Default, alternate and neighboring gatekeeper management
- Device registration
- Address resolution
- Bandwidth control and management
- Call control signaling
- Call management, authorization, access, and accounting
- Firewall traversal

Default, Redundant, Alternate, and Neighboring Gatekeepers

Default Gatekeeper

We recommend setting up the Polycom CMA system as the default gatekeeper, so that all endpoints on the network capable of automatic registration will register with the same gatekeeper. This allows the Polycom CMA system gatekeeper to serve as the centralized manager of the H.323 network and more effectively aid in bandwidth management, firewall traversal, and device authentication and authorization.

Redundant Gatekeeper

When the Polycom CMA system is deployed in a redundant configuration, the redundant gatekeeper runs in parallel with the primary gatekeeper sharing endpoint registration information. If the primary gatekeeper becomes unavailable, the redundant gatekeeper replaces it until it returns.

Alternate Gatekeeper

Within the Polycom CMA system, you can designate an alternate gatekeeper. In this case, when an endpoint registers with the Polycom CMA system gatekeeper, the system sends back the alternate gatekeeper information to the endpoint. Then, if communication with the Polycom CMA system fails, the endpoint will attempt to register with the alternate gatekeeper.

In a redundant configuration, the alternate gatekeeper is the third gatekeeper in line after the primary and redundant Polycom CMA system gatekeepers.

Neighboring Gatekeeper

Neighboring gatekeepers are gatekeepers that manage other H.323 regions within an enterprise. When a call originates within one gatekeeper region but that region's gatekeeper is unable to resolve the dialed address, it is forwarded to the neighboring gatekeepers for resolution.

Within the Polycom CMA system, you can also set up a dial rule that will route calls with designated prefixes to designated neighboring gatekeepers.

Device Registration

The Polycom CMA system manages device registration and offers several choices from an open registration policy to more restrictive registration policies.

No matter what the gatekeeper registration policy, any endpoint that is automatically provisioned, any endpoint that is registered with the Global Address Book, and any endpoint that is added manually to the Polycom CMA system can automatically register with the gatekeeper.

The Polycom CMA system gatekeeper registration policies include:

Allow Registration of All Endpoints

This open **Allow Registration of All Endpoints** registration policy allows any device that can find the Polycom CMA system gatekeeper to register with it. This is the default policy.

In this case, devices can register to the Polycom CMA system automatically:

- When the device broadcasts a message to find a gatekeeper with which to register.

In this case, specifying a default gatekeeper is important, because devices that register automatically may find multiple gatekeepers. Devices register with the system designated as the default gatekeeper, unless that gatekeeper is down. Then devices register with the system designated as the alternate gatekeeper.

When registering, devices send a variety of settings to the gatekeeper including their IP address, one or more H.323 IDs, and one or more E.164 aliases. These settings appear in the Polycom CMA system as **Device Details**.

- When devices in dynamic management mode are automatically provisioned by the Polycom CMA system

And devices can be registered to the Polycom CMA system manually:

- At the device by specifying the IP address of the Polycom CMA system as the gatekeeper
- At the device by specifying the IP address of the Polycom CMA system as the Global Directory Service. Once the device in in the Polycom CMA system Global Address Book it is registered to the system.
- At the Polycom CMA system by adding the device to the one of the device lists (Endpoint, MCU, VBP, or DMA lists)

Once an endpoint is registered, users of other registered endpoints can call the endpoint by using either the H.323 ID, a URI, an E.164 alias, or one of the services.

Allow Registration of Predefined Endpoints Only

The restrictive **Allow Registration of Predefined Endpoints Only** registration policy allows devices to automatically register once they are added to the Polycom CMA system either when they are automatically provisioned, automatically registered to the Global Address Book, or added to the system manually.

Allow Registration of Endpoints in Defined Sites

The moderately open **Allow Registration of Endpoints in Defined Sites** registration policy allows endpoints to automatically register if they are within one of the Dial Plan sites defined to the Polycom CMA system, when they are automatically provisioned, when they are automatically registered to the Global Address Book, or when they are added to the system manually

Allow Registration of Predefined Prefixes Only

With this controlled registration policy, devices within a range of defined E.164 prefixes may automatically register with the Polycom CMA system.

Routing Mode

The Polycom CMA system has two routing modes.

Direct Mode

In this simplest gatekeeper mode, the Polycom CMA system gatekeeper resolves IP addresses to their E.164 addresses and Aliases (similar to the function of a domain name server) and grants endpoints permission to place calls. Once the gatekeeper performs these two functions, it plays no further role in the call. Call signaling and media streams are sent directly between the endpoints in the call.

In **Direct** mode, the number of concurrent calls supported by a Polycom CMA system is derived from the number of device licenses at a 3/5 ratio (calls/devices). So, for example, a system in **Direct** mode licensed for 5000 devices supports up to 3000 calls.

Use **Direct** mode when implementing a hierarchical architecture. A hierarchical architecture is one with multiple gatekeepers, where one gatekeeper—the Polycom CMA system in **Direct** mode—acts as the directory gatekeeper at the top of the hierarchy. On the directory gatekeeper, you must configure all of the other member gatekeepers as neighbors and on the member gatekeepers you must configure the directory gatekeeper as a neighbor. However, the member gatekeepers do not have to be neighbored with each other.

When in **Direct** mode, some advanced Polycom CMA system features do not work. These features include Simplified Dialing, Conference on Demand, Alternate Routing, Least Cost Routing, MCU board hunting, and firewall traversal for a Polycom VBP system in "Enterprise" or "E" mode. (Firewall traversal for a Polycom VBP system in "Service Provider or "S" mode does work.)

The advantage of **Direct** mode is that conferences stay connected even if the gatekeeper fails.

The disadvantage of **Direct** mode (along with the loss of advanced functionality) is that during a failure and restart the gatekeeper loses track of active calls that it was not involved in setting up. In this case, after a failure and restart, the gatekeeper's bandwidth calculations will be incorrect until those calls end. Also, since the Conference Monitoring function uses gatekeeper data, the monitoring information for those calls may be incorrect or incomplete.

Routed Mode

In this advanced mode, the Polycom CMA system gatekeeper, besides performing the functions of a **Direct** mode gatekeeper, also acts as a proxy for the call signaling H.225 messages that set up the call. In this mode, only the media streams are sent directly between the endpoints in the call.

In **Routed** mode, the number of concurrent calls supported by a Polycom CMA system is derived from the number of device licenses at a 3/10 ratio (calls/devices). So, for example, a system in **Routed** mode licensed for 5000 devices supports up to 1500 calls.

The advantage of **Routed** mode is that it enables advanced features such as Simplified Dialing, Conference on Demand, Alternate Routing, Least Cost Routing, MCU board hunting and firewall traversal for a Polycom VBP system in "Enterprise" or "E" mode. Routed mode is also supported for the Polycom VBP system in "Service Provider" or "S" mode.

The disadvantage of routed mode is that a gatekeeper failure and restart terminates all running conferences that include a registered devicec. Calls are not reestablished after a system failure and restart. Conferences show a status of **Active**, but participants show a status of **Disconnected**.

In either mode, CDR information for calls is accurate if the Polycom CMA system does not fail and the endpoints send a DRQ (Disconnect Request) at the end of the call.

25

Server Setting Operations

This chapter describes how to update the Polycom® Converged Management Application™ (CMA™) system configuration settings, many of which were entered during **First Time Setup**. It includes these topics:

Edit the Polycom CMA System Network Settings

Edit the system **Network** settings to change the basic network information for the Polycom CMA system. Network settings include these fields:

To edit the Polycom CMA system network settings

1 Go to **Admin > Server Settings > Network**.

2 Configure these settings on the **Network** page, as necessary.

Field	Description
System Name	The NetBIOS name (ASCII only[a]) of the Polycom CMA system server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.
IP Address	The static IP address for the Polycom CMA system server
Subnet Mask	The network subnet mask for the Polycom CMA system IP address
Default Gateway	The static IP address of the Polycom CMA system gateway
DNS Server	The IP address of the domain name server for the network
DNS Domain	The fully qualified domain for network in which the domain name server and Polycom CMA system server reside

a. For more information on field limitations, see "Field Input Requirements" on page 6.

3 Click **Update**.

If you change the IP address, the system prompts you to restart the Polycom CMA system . We also recommend that you restart the system if you change the subnet mask.

Note

Changing the IP address via the **Windows Network Settings** is not a supported operation. To change the Polycom CMA system IP address, you must use this procedure.

4 As required, restart the system.

Edit the Polycom CMA System Time Settings

Edit the **System Time** server settings to change the Polycom CMA server time or to synchronize the server with an external NTP server. The system time settings include these fields:

To edit the Polycom CMA system time settings

1 Go to **Admin > Server Settings > System Time**.

2 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the Polycom CMA server resides
Auto adjust for Daylight Saving?	Select this checkbox to adjust the clock automatically for daylight savings time.
Use Current Time	Select this checkbox to input the current date and time.
Current Date	The system date for the Polycom CMA system
Current Time	The system time for the Polycom CMA system
Use External NTP Server Time Synchronization	Select this checkbox to synchronize the Polycom CMA system date and time with an external NTP server.
IP address or DNS resolved name	The IP address or fully qualified domain name (ASCII only[a]) of the NTP server
Minutes between synchronization attempts	Input how often the Polycom CMA system should synchronize with the NTP server The default is 60 minutes.

a. For more information on field limitations, see "Field Input Requirements" on page 6.

Notes

- Make sure the current system time is correct before synchronizing with an NTP server. If you set the system to use an external NTP server when the current date and time are incorrect, the system time may be wrong for the amount of time specified in the **Minutes between synchronization attempts**.
- If the Polycom CMA system is already running when you connect to an NTP server for the first time, you must restart the Polycom CMA system to ensure the time is synchronized correctly.

3 Click **Update**.

Integrate the Polycom CMA System to an External Database

Polycom CMA 5000 systems require an external database. An external database is optional for Polycom CMA 4000 systems.

To integrate the Polycom CMA system to an external Microsoft SQL Server, edit the **Database Integration** server setting.

Some information about using an external database:

- If you set up an external database, follow your own corporate policies (or Microsoft best practices) to back it up and maintain it. The Polycom CMA system does not backup external databases.
- We recommend that anytime you reboot the external database server, you also restart the Polycom CMA system in the same maintenance window.
- You can create the Polycom CMA system databases manually using Microsoft SQL scripts. Contact Polycom Global Services to request the scripts.

To integrate Polycom CMA with an external database

1 Go to **Admin > Server Settings > Database**.

2 On the **Database** page, select **Use an external SQL Server database**.

Note

If this is not the first time you've integrated with an external database on this server, and you wish to preserve the existing database, skip the **Database Setup** steps 3 and 4.

3 Click **Database Setup** and download the **Remote Database Setup Utility**, `DBSetup.exe`, to your computer.

Note

If you are installing a redundant Polycom CMA system configuration, perform step 4 on the primary server only. When performing this procedure on the secondary server, skip to step 5.

4 Run the **Remote Database Setup Utility** and complete the information requested in the setup pages.

   – Make sure you know the path to the Microsoft SQL server.

   – If you use Microsoft Windows authentication, be sure the login ID has administrator privileges on the SQL server.

   – If you use Microsoft SQL authentication, be sure the login ID is a member of the `sysadmin` role.

- If a Polycom CMA system database was installed previously on the server, make sure you overwrite it.

5 Enter the database server's IP address, SQL server port number, and the database instance name (if necessary, otherwise leave it blank) in the **Database** page. (Note that the database instance name field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

6 Click **Update**.

Revert the Polycom CMA System to the Internal Database

To revert from an external database to the internal database

1 Go to **Admin > Server Settings > Database**.

2 On the **Database** page, uncheck **Use an external SQL Server database** and click **Update**.

Note

To go back to the external database, follow the procedure to "Integrate the Polycom CMA System to an External Database" on page 250, but DO NOT run the Database Setup (steps 3 and 4), or you will overwrite the existing database.

Integrate the Polycom CMA System to an Enterprise Directory

To allow Polycom CMA system users to select conference participants and rooms from your company's enterprise directory, you must integrate the Polycom CMA system with a Microsoft Active Directory implementation of an LDAP directory. To do this, you must edit the **LDAP** server settings.

Note

To allow endpoints to use NTLM Single Signon technology to connect to the Polycom CMA system and access services such as automatic provisioning, automatic softupdate, and presence, see "Use Integrated Windows Authentication" on page 253.

To integrate the Polycom CMA system to an enterprise directory, the system requires an account that has read access to all domains in the Active Directory.

To integrate the Polycom CMA system to an LDAP server

1 Go to **Admin > Server Settings > LDAP**.

2 On the **LDAP** page, select **Integrate with LDAP server**.

3 Enter the **LDAP Server IP Address or DNS Name**.

Note

When entering the **DNS Name** of the LDAP server:

- Enter the fully qualified domain name e.g., <*server.domain.com*>
- Use ASCII only. For more information, see "Field Input Requirements" on page 6.

4 Enter the **Domain\LDAP User ID** and **Password** required to access the LDAP server.

Notes

- This User ID must have read access to all of the domains managed by the LDAP server.
- This User ID is automatically associated to a Polycom CMA Administrator role.

5 To exclude disabled users from searches, select **Ignore Disabled AD users**.

6 If necessary and you understand LDAP filter syntax, in the **LDAP Exclusion Filter** field specify which user accounts to exclude. (An underlying, non-editable filter excludes all non-user objects in the directory.)

7 If necessary and you understand LDAP filter syntax, in the **LDAP Search Base DN** field, specify the top level of the LDAP directory tree (referred to as the base DN) to search.

Note

Don't edit these expressions unless you understand LDAP filter syntax.

8 Click **Update**.

Use Integrated Windows Authentication

To allow dynamically-managed endpoints to use NTLM Single Signon technology to connect to the Polycom CMA system and access services such as automatic provisioning, automatic softupdate, and presence, you must enable Windows authentication on the Polycom CMA system.

The Polycom CMA system requires an account that has read access to all domains in the Active Directory.

Notes

- To enable Windows authentication on the Polycom CMA system an Active Directory administrator must provide credentials. These credentials are required to create a trusted machine account so that the Polycom CMA system can perform trusted passthrough authentication.
- To allow Polycom CMA system users who enter their network usernames and passwords to log into the Polycom CMA system and select conference participants from your company's active directory, see "Integrate the Polycom CMA System to an Enterprise Directory" on page 251.

To enable an active directory domain controller

1. Go to **Admin > Server Settings > LDAP**.
2. On the **LDAP** page, select **Use Integrated Windows Authentication**.
3. Enter the **Domain controller name** for the Active Directory domain controller. This is the fully qualified hostname of the domain controller (for example, dc1.mydomain.com).
4. Click **Update**.

   A dialog box appears prompting you to enter a valid Active Directory administrator username and password.
5. Enter the proper credentials and click **OK**.

View Current Polycom CMA System Licensing

To view current Polycom CMA system licensing

>> Go to **Admin > Server Settings > Licenses**.

The **Active License** section of the **Licenses** page displays the following information.

Field	Description
Activation Key	The current activation key for the product.
Expiration date	The expiration date of the current license key.
Components	The components for which the Polycom CMA system is licensed. Possible values include:
Seats	The number of seats for which the Polycom CMA system is licensed. Possible values include:

Add Polycom CMA System Licenses

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

- Request a Software Activation Key Code.
- Enter the Polycom CMA System Activation Key

These processes are described in the following sections.

Request a Software Activation Key Code

To request a software activation key code

1. In a separate browser page or tab, log into the Polycom CMA system server as an administrator.
2. Go to **Admin > Server Settings > Licenses** and record the Polycom CMA server serial number:

   _____.
3. Go to **http://www.polycom.com/activation**.
4. Log in or **Register for an Account**.
5. Select **Product Activation**.

6 In the **Single License Number** section of the **Activate Your Product** page, enter the software license number listed on your License Certificate (shipped with the product) and the serial number you recorded in step 2.

7 Click **Generate**.

8 When the activation key appears, record it:

_____-_____-_____-_____

9 Repeat this procedure for each additional license key required.

Enter the Polycom CMA System Activation Key

To enter the Polycom CMA system activation key

1 Go to **Admin > Server Settings > Licenses**.

2 Enter the new activation key into the **Add New License > Activation Key** field and click **Add**. (Note that the field is ASCII only. For more information, see "Field Input Requirements" on page 6.)

The license number appears in the list and the number of active licenses is updated.

Reclaim Polycom CMA Desktop Licenses

To set the threshold for reclaiming inactive Polycom CMA Desktop licenses

1 Go to **Admin > Server Settings > Licenses**.

2 Change the **Threshold** value in the **Reclaim Inactive CMA Desktop Licenses** section of the **Licenses** page. To reclaim licenses more quickly, lower the threshold. Set the threshold to zero, to stop reclaiming licenses.

3 Click **Update**.

Delete Polycom CMA System Licenses

To delete Polycom CMA Desktop licenses

1 Go to **Admin > Server Settings > Licenses**.

2 In the **Active License** section of the **Licenses** page, select the component of interest and click **Delete**.

3 Click **Delete** to confirm the deletion.

Add a Custom Logo to the Polycom CMA System Interface

You can add your company's logo to the Polycom CMA system user interface. To avoid distortion, we recommend adding a logo in GIF, JPG, or PNG format with a size of 300 x 44 pixels.

To add a custom logo to the Polycom CMA system user interface

1 Go to **Admin > Server Settings > Custom Logos**.

2 In the **Current Server Logo** section of the **Custom Logos** page, click **Upload...**

3 In the **Select file** dialog box, browse to the logo image and select the file.

4 Click **Open**.

5 In a redundant configuration, repeat steps 1 through 4 on the redundant server.

To remove a custom logo

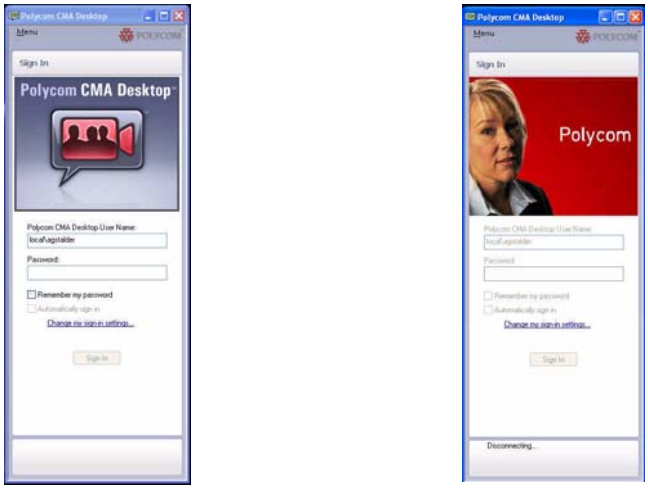
1 Go to **Admin > Server Settings > Custom Logos**.

2 In the **Current Server Logo** section of the **Custom Logos** page, click **Remove**.

Add a Custom Logo to the Polycom CMA Desktop Interface

You can add your company logo to the Polycom CMA Desktop user interface. This logo will be displayed on the application user interface before the user logs in. The following illustration shows the default Polycom CMA Desktop user interface and a customized Polycom CMA Desktop user interface.

Default Polycom CMA Desktop **Branded Polycom CMA Desktop**



To avoid distortion, use a logo in GIF or JPG format with a size of approximately 260x215 pixels.

Because the Polycom CMA Desktop logo is stored in the Polycom CMA system database, in redundant configurations you do not need to upload the logo to both servers.

To add a custom logo Polycom CMA Desktop user interface

1. Go to **Admin > Server Settings > Custom Logos**.
2. In the **Current CMA Desktop Logo** section of the **Custom Logos** page, click **Upload...**
3. In the **Select file** dialog box, browse to the logo image and select the file.
4. Click **Open**.

   Once a user logs in, is provisioned, and then logs out, the logo will be displayed on the Polycom CMA Desktop user interface.

To remove a custom logo

1 Go to **Admin > Server Settings > Custom Logos**.

2 In the **Current CMA Desktop Logo** section of the **Custom Logos** page, click **Restore Default**.

Once a user logs in, is provisioned, and then logs out, the default logo will be displayed on the Polycom CMA Desktop user interface.

Include Enterprise Users in the Global Address Book

You may choose to include all enterprise users from the active directory in the Global Address Book. This brings all of your users together into one directory.

> **Note**
> You may not want to take advantage of this feature if you have legacy devices such as VSX, ViewStation, and FX endpoints. These devices may not be able to handle the size of the Global Address Book.

To include enterprise users in the Polycom CMA system Global Address Book

1 Go to **Admin > Server Settings > Global Address Book**.

2 In the **Global Address Book** page, select **Include all the Active Directory Users in the Global Address Book**.

3 Click **Update**.

Edit the Polycom CMA System Email Account

To edit the Polycom CMA system email account

1 Go to **Admin > Server Settings > E-mail**.

2 On the **Email** page, edit the email account (ASCII only) from which the Polycom CMA system will send conference notification emails or edit the IP address of the mail server from which the Polycom CMA system will send conference notification emails.

Notes

- Many E-mail servers will block or discard emails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid email address.
- Many E-mail servers will block or discard emails from un-trusted domains, in which case you may need to change the default Polycom CMA system email address to one in a trusted domain.

3 Click **Update**.

26

Polycom CMA System Redundancy

This chapter describes how to configure a redundant Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Polycom CMA 5000 System Redundancy Overview

A redundant Polycom CMA system configuration offers higher reliability and greater call success by ensuring that a Polycom CMA system server is always available.

A redundant Polycom CMA system configuration requires two Polycom CMA system servers and three IP addresses on the same network—one physical IP address for each of the servers and one virtual IP address dedicated to endpoint registration.

How Redundancy Works

In a redundant configuration:

- One Polycom CMA server is designated the primary server and the other is designated the redundant server. Each server must be licensed. The licenses identify which server is the primary server and which is the redundant server.

- The two servers share the external Polycom CMA system database, so what is recorded by one Polycom CMA system is read by the other Polycom CMA system. An external Microsoft SQL Server database is required.
- If the primary server goes down for any reason, the system fails over and the redundant server takes over. Note that failures in services do not initiate a failover, only a server failure.
- An administrator can force a failover via the **Switch Server Roles** function in the Polycom CMA system user interface. Failover does not require a system restart.
- The Polycom CMA database information—call records, endpoint registration information, and network topology configurations—remains consistent and available during a failover because both servers point to the same database.
- The failover to the redundant server seems to occur seamlessly because the endpoints are registered with the virtual IP address, which remains constant.

During a system failover, which takes approximately 5 minutes:

- Active conferences are dropped from the system. Conference participants can call back in using the same conference information.
- Users logged into the Polycom CMA system user interface are disconnected and returned to main Polycom CMA system web page. Users can log back in once failover is completed.
- Users in the middle of an operation may get an error message, because the system is not available to respond to a request.

Some system settings affect how rapidly a redundant system returns to full functionality. The gatekeeper **Registration Timeout** and **Registration Refresh** affect how quickly endpoints re-register with the redundant server after a failover. And if **Deny calls to/from unregistered endpoints** is checked, the gatekeeper rejects calls from endpoints that have not re-registered with the redundant server after a failover. Therefore, in a redundant system configuration, use a short refresh period (30 seconds) unless you have many endpoints or a large amount of network traffic.

Once a failover to a redundant server occurs, the redundant server manages all system operations until an administrator switches back to the original primary server via the **Switch Server Roles** function in the Polycom CMA system user interface.

Notes

- The Polycom CMA system does not automatically switch to the primary server when the primary server becomes available. An administrator must **Switch Server Roles**.
- A failover or system restart initiates an encryption routine that changes the private key for a redundant system. Therefore, after a failover or system restart, schedulers who use one of the scheduling plug-ins will be prompted to re-enter their login settings to access the system.

Redundant Configuration System Administration

Because the two servers share the external Polycom CMA system database, most of their configuration information is shared. However, certain information is not stored in the database, so an administrator must manually synchronize this information. This includes:

- Basic network settings such as IP, default gateway, and DNS server settings
- External database information
- Time and external NTP server settings
- The common device management password
- The current system log level
- Custom Polycom CMA system logo--upload the same logo to both servers
- Softupdate profiles for scheduled softupdates--upload the same software package to both servers

Whenever you change information in one of these sections on one server you should also change it on the other server.

Licensing and upgrading a redundant system is slightly more complex. The primary and redundant server required different licenses.

Implement a Redundant Polycom CMA 5000 System

You can set up a Polycom CMA 5000 system in a fault-tolerant, high-availability, redundant configuration. The Polycom CMA 4000 system is not available in a redundant configuration.

A redundant Polycom CMA 5000 system configuration requires two Polycom CMA 5000 system servers on the same network. It also requires an external Microsoft SQL Server database.

This section describes how to convert an existing non-redundant Polycom CMA 5000 system to a redundant configuration.

To add a redundant Polycom CMA system server to an existing system

1. Install the redundant Polycom CMA 5000 system as described in the *Polycom CMA Getting Started Guide*. During installation, point the redundant Polycom CMA 5000 system server to its internal database.
2. Request the required software activation key code for the redundant server as described in "Request a Software Activation Key Code" on page 254.
3. Log into both the primary and redundant Polycom CMA 5000 system servers.
4. Point the primary server to an external Microsoft SQL Server database and re-enter the license as described in "Integrate the Polycom CMA System to an External Database" on page 250.
5. On the primary server:
   a. Go to **Admin > Server Settings > Redundant Configuration**.
   b. Enter the **Virtual IP** for the redundant system and click **Submit**.
6. On the redundant server:
   a. Go to **Admin > Server Settings > Database**.
   b. On the **Database** page, select the **Use an external SQL Server database** check box.
   c. Enter the database information from the primary server i.e., the database server's IP address, SQL server port number, and the database instance name (if necessary, otherwise leave it blank) in the **Database** page. (Note that the **Database Instance Name** field is ASCII only. For more information, see "Field Input Requirements" on page 6.)
   d. Click **Update**.

      The Polycom CMA 5000 system connects to the database server and the redundant server restarts and comes online.
7. On the primary server, fail over to the redundant server. See "Failover to a Redundant Polycom CMA 5000 System Server" on page 268.
8. Once the failover is complete, on the redundant server:
   a. Log into the Polycom CMA 5000 system *using the virtual IP address*, and go to **Admin > Server Settings > Licenses**.
   b. Enter the activation key code for the redundant server into the **Add New License > Activation Key** field and click **Add**. (Note that the field is ASCII only. For more information, see "Field Input Requirements" on page 6.)
   c. Go to **Admin > Dashboard** and click **Restart**  to restart the system.

      This system fails over to the primary server.

You can install the Polycom CMA 5000 system in a fault-tolerant, high-availability, redundant configuration. The Polycom CMA 4000 system is not available in a redundant configuration.

A redundant Polycom CMA system configuration requires the installation of two Polycom CMA system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses and leave them pointed at their internal databases. This section describes how to complete the configuration of these newly installed redundant servers. It includes these topics:

1 Configure the External Database for Redundancy

2 Set the Virtual IP Address for the Redundant System

Note

This procedure describes implementing a new redundant Polycom CMA system. For information on converting an existing system to a redundant system, see "Add a Custom Logo to the Polycom CMA System Interface" on page 256.

Configure the External Database for Redundancy

To configure the two redundant servers to use the same external database

1 Log into both the primary and redundant Polycom CMA 5000 system servers.

2 On the primary server, go to **Admin > Dashboard** and click **Shutdown** to shut down the primary server.

3 When the primary server has shutdown completely, on the redundant server:

   a Go to **Admin > Server Settings > Database**.

   b On the **Database** page, select the **Use an external SQL Server database** check box.

   c Click **Database Setup** and download the **Remote Database Setup Utility**, `DBSetup.exe`, to your computer.

   d Run the **Remote Database Setup Utility** and complete the information requested in the setup pages.

      » Make sure you know the path to the Microsoft SQL Server.

      » If you use Microsoft Windows authentication, be sure your login account has administrator privileges on the SQL server (i.e., is a member of the `sysadmin` group).

   After running the script, the redundant server boots.

   e After the redundant server restarts completely, log into it again and select **Admin > Dashboard**.

f Click **Shutdown** to shut down the redundant server.

4 When the redundant server has shutdown completely, on the primary server:

a Turn ON the primary server.

b Log into the server and go to **Admin > Server Settings > Database**.

c On the **Database** page, select the **Use an external SQL Server database** check box.

d Enter the database server's IP address or host name, SQL server port number, and the database instance name (if necessary, otherwise leave it blank).

e Click **Update**.

The primary server restarts and comes online as the primary server.

5 When the primary server has restarted completely, turn ON the redundant server and wait for it to boot completely.

Set the Virtual IP Address for the Redundant System

To set the virtual IP address for the redundant system

1 Log into the primary Polycom CMA 5000 system server.

2 Go to **Admin > Server Settings > Redundant Configuration**.

If the two Polycom CMA system servers are installed and configured correctly on the network, both servers are displayed in the table on the **Redundant Configuration** page.

3 Enter the **Virtual IP** for the redundant system and click **Submit**. For information about this virtual IP address, see "Add a Custom Logo to the Polycom CMA System Interface" on page 256.

Note
Set the virtual IP for the redundant server on the primary server only.

License a Redundant Polycom CMA System

To license a non-redundant Polycom CMA system, see "Add Polycom CMA System Licenses" on page 254. This section describes how to license a redundant system.

To license a redundant Polycom CMA 5000 system

1. Request a separate software activation key code for the primary and redundant server as described in "Request a Software Activation Key Code" on page 254.
2. On the primary Polycom CMA 5000 system server:
   a. Go to **Admin > Server Settings > Database** and verify the database information. (If you fail to point the server to the correct database, you must re-enter the license when you change databases.)
   b. Go to **Admin > Server Settings > Licenses**.
   c. Enter the activation key code for the primary server into the **Add New License > Activation Key** field and click **Add**.

      The license number appears in the list and the number of active licenses is updated.
   d. Go to **Admin > Server Settings > Redundant Configuration**. and click **Switch Server Role**.

      The system fails over to the redundant server.
3. On the redundant server:
   a. Log into the Polycom CMA system *using the virtual IP address*, and go to **Admin > Server Settings > Licenses**.
   b. Enter the software activation key code for the redundant server into the **Add New License > Activation Key** field and click **Add**.
   c. Go to **Admin > Dashboard** and click **Restart**  to restart the system.

      The system fails over to the primary server.

Failover to a Redundant Polycom CMA 5000 System Server

In a redundant configuration, the Polycom CMA 5000 system automatically fails over from the primary server to the redundant server. However, you can also manually initiate a failover.

To manually initiate a failover

1. On either server, go to **Admin > Server Settings > Redundant Configuration**.
2. On the **Redundant Configuration** page, click **Switch Server Role**.

   The system initiates a failover to the other server.

Discontinue Redundancy on a Polycom CMA 5000 System Configuration

In some circumstances, you may need to discontinue redundancy. Use this procedure to do so, but only when the system is in a valid redundant state.

To discontinue a redundant Polycom CMA 5000 system configuration:

1. Log into the Polycom CMA 5000 system *using the virtual IP address*.
2. Failover to the redundant server. See page 268.
3. On the redundant server:
   a. Go to **Admin > Server Settings > Database**.
   b. On the **Database** page, deselect the **Use an external SQL Server database** check box.
   c. Click **Update**.

      The redundant server restarts.
4. On the primary server:
   a. Go to **Admin > Server Settings > Redundant Configuration**.
   b. On the **Redundant Configuration** page, click **Reset Redundant Configuration**.

      The primary system restarts.

27

Gatekeeper Management

This chapter describes how to work with gatekeepers within the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

Gatekeeper Overview

The Polycom CMA system gatekeeper provides address translation and network access control services for endpoints, gateways, and MCUs. It also provides other services such as bandwidth management and dial plans services. These additional features allow you to configure and manage your gatekeeping operations and provide flexibility and scalability.

During **First Time Setup**—the Polycom CMA system's initial configuration—the system is assigned a default region and site (called **My Region: Primary Site**). A region is just the set of network devices that share a common Polycom CMA system gatekeeper, so a gatekeeper has only a single region or zone. However, a region or zone can have multiple sites.

This initial set up allows you to immediately start using the Polycom CMA system for video conferencing. However, you can also configure the system may change the name of the default site and assign the sites you have created. You may create additional neighboring gatekeeper regions, if needed. When you create a new gatekeeper region, you define gatekeeper settings only. A gatekeeper region functions as a neighboring gatekeeper. You cannot add sites to a newly created gatekeeper region.

When a call originates from the Polycom CMA system and the system is unable to resolve the dialed address, the call can be forwarded to another gatekeeper for resolution. To enable call forwarding, create a neighboring region and a dialing rule that routes calls using a particular prefix to the neighboring gatekeeper.

If you have a Polycom PathNavigator installed, it can act as a neighboring gatekeeper region to the Polycom CMA system.

Note
To prevent a site from participating in a dial plan, do not assign it to a region.

Field	Description
Name	The name (ASCII only[a]) of the region.
Description	A description (ASCII only[a]) of the region.
Gatekeeper IP Address	The IP address for this region. For the default region, automatically set to the IP address of the Polycom CMA system server.
Port	The port for this region. Defaults to the port for the Polycom CMA system server.
Gatekeeper Identifier	The unique ID (ASCII only[a]) for the gatekeeper associated with this region. Automatically filled in for the default region. PN: is inserted in front of the gatekeeper identifier. Example: `PN: Silicon Valley Campus` The character limit is 254; all keyboard characters are supported.”

a. For more information, see .

Primary Gatekeeper Management Operations

By default the Polycom CMA system is made the primary gatekeeper during the **First Time Setup** process. Operations for managing the primary gatekeeper include:

- Edit the Primary Gatekeeper Settings
- Configure Prefixed Based Registration

Edit the Primary Gatekeeper Settings

To edit the primary Polycom CMA system gatekeeper settings

1 Go to **Admin > Gatekeeper Settings > Primary Gatekeeper**.

2 On the **Primary Gatekeeper** page, make the required changes.

The **Primary Gatekeeper Settings** include these fields:

Field	Description
Gatekeeper Identifier	The gatekeeper identifier (ASCII-only[a]) on the network, which is used by the endpoints and Polycom CMA system for communication. The maximum number of characters is 254. All ASCII characters are valid.
Gatekeeper Description	The description (ASCII only[a]) of this gatekeeper on the network
Default Gatekeeper	When enabled, indicates that this Polycom CMA system is the default gatekeeper on the network
Allow Registration of	Defines for the gatekeeper of which endpoints to allow to register. • **All Endpoints.** An open gatekeeper registration policy that allows any device that can register with the Polycom CMA system to do so automatically. With this policy, any device and the registration settings entered at the device automatically appear in the device list. This is the default policy. • **Predefined Endpoints Only.** With this secure gatekeeper policy, devices are automatically added to the device list via the Global Address Book. • **Endpoints in Defined Sites**. With this moderately open registration policy, devices at identified Polycom CMA system sites may automatically register with the Polycom CMA system. • **Predefined Prefixes Only**. With this controlled registration policy, devices within a range of defined E.164 prefixes may automatically register with the Polycom CMA system.

Field	Description
Registration Timeout (day)	The number of days that the Polycom CMA gatekeeper maintains the endpoint registration information, in case the endpoint has not yet received any. The default is 30 days. Enter 999 to prevent endpoint registrations from expiring automatically.
Registration Refresh (seconds)	The interval at which the Polycom CMA system sends “keep-alive” messages to registered endpoints to determine whether they are online. The default is 300 seconds. If the endpoint responds with a registration request message, the endpoint is online. If not, the endpoint is offline. When the endpoint is registered to another gatekeeper, the Polycom CMA system still shows the endpoint’s status. To view the endpoint’s state (**Online** or **Offline**), go to **Endpoint> Monitor View**. **Note** Endpoints are **Offline** when they have been turned off or have been removed from the network. Endpoints return to an **Online** state when they have been turned on or have reregistered with Polycom CMA system.
Maximum Neighbor Gatekeeper Hop Counts	Limits the number of connections to make when an endpoint seeks dialing resolution. The default is 3.
Log calls to/from unregistered endpoints	Logs calls to and from rogue endpoints. To view call logs, select **System Management > Reports > Gatekeeper Message Log**.
Deny calls to/from unregistered endpoints	Prevents calls to and from rogue endpoints.
IRR frequency	The frequency of the gatekeeper’s response to the calling or receiving endpoint. The default is 0.
Call Model	Describes how the Polycom CMA system routes selected H.225 call signalling messages (i.e., SETUP, CALL PROCEEDING, ALERTING, CONNECT, and NOTIFY message). Possible values include: **Routed** or **Direct**. For more information, see . In any case, Q.931 messages (ARQ, ACF, ARJ, BRQ, BCF, and BRJ) are always sent through the Polycom CMA system gatekeeper.

a. For more information, see .

3 Click **Update**.

Configure Prefixed Based Registration

A user with administrator permissions can configure the Polycom CMA system so that only endpoints with specified E.164 prefixes are allowed to register to the H.323 gatekeeper.

Note that when you apply this policy to an system with existing endpoints, all existing endpoints that fail to meet the new policy will fail to re-register with the gatekeeper. This will be flagged in the **Endpoint > Monitor View** as a gatekeeper registration error.

To allow only the registration of endpoints with defined E.164 prefixes

1 Go to **Admin > Gatekeeper Settings > Primary Gatekeeper**.

On the **Primary Gatekeeper** page, change the **Allow Registration of** setting to **Predefined Prefixes Only**.

The **Valid E.164 Prefixes** entry box appears.

2 Enter a range of prefixes in the **From** and **To** fields and click **Add**.

The prefix range appears in the **Allowed Prefix Ranges** table.

3 Continue adding prefixes ranges as necessary. To delete a range, select the range and click the **Delete** button for it.

When you've specified all the prefix ranges, click **Update**.

Alternate Gatekeeper Management Operations

Alternate Gatekeeper Management Operations include:

- Add an Alternate Gatekeeper
- Edit the Alternate Gatekeeper Settings
- Remove the Alternate Gatekeeper

Add an Alternate Gatekeeper

To add an alternate gatekeeper

1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.

2 On the **Alternate Gatekeeper** page, enter the required gatekeeper information.

The **Alternate Gatekeeper Settings** include these fields:

Field	Description
Need to Register	Check this box to require that a device register with the alternate gatekeeper before sending other registration admission status requests.The default setting is unchecked.
Alternate Gatekeeper ID	The alternate gatekeeper's network identifier (ASCII only[a])
IP Address	The IP address of the alternate gatekeeper
Port	The port number (usually 1719) that the alternate gatekeeper uses to communicate with endpoints
Priority	Indicates the alternate gatekeeper's priority for endpoint registration. A lower number has higher priority (the range is 0 to 127), so endpoints would first register with an alternate gatekeeper with a priority of 0. The default setting is 0.

a. For more information, see .

3 Click **Update**.

Edit the Alternate Gatekeeper Settings

To edit the alternate gatekeeper settings

1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.

2 On the **Alternate Gatekeeper** page, make the required changes. For more information, see **Alternate Gatekeeper Settings**

3 Click **Update**.

Remove the Alternate Gatekeeper

To remove the alternate gatekeeper settings

1 Go to **Admin > Gatekeeper Settings > Alternate Gatekeeper**.

2 On the **Alternate Gatekeeper** page, clear the **Need to Register** checkbox.

3 Click **Update**.

Neighboring Gatekeeper Management Operations

Neighboring Gatekeeper Management Operations include:

- View Neighboring Gatekeepers
- Add a Neighboring Gatekeeper
- Edit a Neighboring Gatekeeper
- Delete a Neighboring Gatekeeper

View Neighboring Gatekeepers

To view the neighboring gatekeepers

>> Go to **Admin > Gatekeeper Settings > Neighboring Gatekeepers**.

The **Neighboring Gatekeepers** list appears.

Column	Description
Name	The name of the region
Description	The description of the region

Add a Neighboring Gatekeeper

To add a neighboring gatekeeper

1 Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.

2 On the **Neighboring Gatekeeper** page, click **Add Neighbor**.

3 In the **Add Neighbor** dialog box, enter the required gatekeeper information and click **Save**.

The neighboring gatekeeper is added to the system.

Edit a Neighboring Gatekeeper

To edit the settings for a neighboring gatekeeper

1. Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.
2. On the **Neighboring Gatekeeper** page, select the neighboring gatekeeper of interest and click **Edit Neighbor**.
3. In the **Edit Neighbor** dialog box, make the required changes and click **Update**.

Delete a Neighboring Gatekeeper

To delete a neighboring gatekeeper

1. Go to **Admin > Gatekeeper Settings > Neighboring Gatekeeper**.
2. On the **Neighboring Gatekeeper** page, select the neighboring gatekeeper of interest and click **Delete**.
3. Click **Delete** to confirm the deletion.

28

Management & Security Operations

This chapter describes the Polycom® Converged Management Application™ (CMA™) system management and security tasks. It includes these topics:

Update the Polycom CMA Server Software

To update a Polycom CMA system with a new software patch, complete the following tasks:

1. Download the software upgrade file.
2. Obtain an upgrade key code.
3. Save a back up of the Polycom CMA system databases.
4. Perform the software upgrade.
5. Verify the upgrade.

For more information on performing each of these tasks, see the *Polycom CMA System Upgrade Guide*.

Edit Certificate Settings to Implement HTTPS

By default, the Polycom CMA system uses `http` for its data interchanges. Edit the **Certficate Settings** to implement the `https` protocol, which is a combination of normal `http` interchange over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection.

If you are implementing HTTPS you have the following decisions to make:

Decision...	If yes, then perform these tasks...
Use the Polycom CMA system default key and certificate?	• "Edit Certificate Settings to Implement HTTPS" on page 278
Use your own existing private key and certificate, if your company is self-authorizing?	• "Upload a Private Key" on page 279 • "Upload a Certificate" on page 280 • "Edit Certificate Settings to Implement HTTPS" on page 278
Use a private key and certificate requested by the Polycom CMA system?	• "Generate a Certificate Request" on page 279 • "Upload a Certificate" on page 280 • "Edit Certificate Settings to Implement HTTPS" on page 278

To prepare the Polycom CMA system web server to accept HTTPS connections, you must also create a public key certificate for it. The following table describes the information needed to request a certificate. All fields are required.

Field	Description
Country Name	Two-letter (ASCII only[a]) ISO 3166 country code
State or Province Name	Full name (ASCII only[a])
Locality Name	City (ASCII only[a])
Organization Name	Company Who (ASCII only[a])
Organization Unit Name	Section (ASCII only[a])
Common Name	Server's host name (ASCII only[a])
Email Address	(ASCII only[a])

a. For more information on field limitations, see "Field Input Requirements" on page 6.

Because the key and certificate are stored in the Polycom CMA system database, in redundant configurations you implement HTTPS on the primary server only.

Notes

- The Polycom CMA system always stores the default key and certificate. However, it stores only the last private key generated or uploaded to the system and the last certificate uploaded to the system.
- The uploaded certificate is for HTTPS connectivity only. The other Polycom CMA system TLS interfaces (for the enterprise directory and presence) are supported via self-signed certificates.
- You may receive certificate warnings if the Polycom CMA Desktop client is using HTTPS while the Polycom CMA system is using HTTP.

Generate a Certificate Request

To generate a certificate request on a PolycomCMA system

1. Go to **Admin > Management and Security Settings > Certificate Settings**.
2. Click **Generate Certificate Request**.

   The system displays a warning that "This action will overwrite any previously generated or uploaded private key. "
3. To continue, click **Yes**.
4. Complete the **Certificate Request Data** dialog box.
5. Save the **Certificate Request Data** to a file and submit the file to the Certificate Authority of your choice.

Upload a Private Key

This procedure describes how to upload a private key to a Polycom CMA system. This private key must be an unencrypted RSA key in PEM format, without a password.

To upload a private key to a Polycom CMA system

1. Go to **Admin > Management and Security Settings > Certificate Settings**.
2. Click **Upload Private Key**.

   The system displays a warning that "This action will overwrite any previously generated or uploaded private key. "
3. To continue, click **Yes**.
4. Browse to the private key file location and select the file.
5. Click **Open**.

   An **Upload Successful** dialog box appears.

Upload a Certificate

This procedure describes how to upload a certificate to a Polycom CMA system. This certificate must be in PEM format.

To upload a certificate from a Certificate Authority

1. If necessary, save the certificate file to a PC on the network.
2. Go to **Admin > Management and Security Settings > Certificate Settings**.
3. Click **Upload Certificate**.
4. Browse to the certificate file location and select the file.
5. Click **Open**.

   The certificate is checked against the private key in the database to verify that they match. If they do, an **Upload Successful** dialog box appears. The certificate file is registered. If `https` is already activated, the web server will restart so that it can load the certificate authority.

Edit the HTTPS Security Setting

To edit the `https` security setting on a Polycom CMA system

1. Go to **Admin > Management and Security Settings > Certificate Settings**.
2. On the **Security Settings** page, check **Use HTTPS**.
3. Click **Update**.

   The system displays a warning that this action will restart the web server and all client sessions will be lost
4. Click **Yes** to confirm the update.

   The Polycom CMA system web server restarts.

Revert to the Default Key and Certificate

If you've implemented a certificate from a Certificate Authority, you can revert to the default certificate.

To revert to the default key and certificate

1. Go to **Admin > Management and Security Settings > Certificate Settings**.
2. Click **Revert to Default Certificate**.

3 Click **OK**.

The system displays a warning that this action will restart the web server and all client sessions will be lost

4 Click **Yes** to confirm the change.

The Polycom CMA system web server restarts.

Configure Client Systems to Accept HTTPS Certificate

When you implement HTTPS on the Polycom CMA system, client systems that access the system interface receive the following HTTPS certificate security alert until they are configured to accept the Polycom CMA system HTTPS certificate.

To configure client systems to accept the HTTPS cerficate without errors

1 Add the Polycom CMA system IP address or DNS name to the DNS server `hosts` file.

2 Instruct client users to install the Polycom CMA system HTTPS certificate as follows:

a Open a browser window and in the **Address** field enter the Polycom CMA system server IP address or DNS name.

b In the **HTTPS Security Alert** page, click **View Certificate**.

c In the **General** tab of the **Certificate** dialog box, click **Install Certificate**.

d When the **Certificate Import Wizard** appears, click **Next**

e Click **Next** again, to accept the default setting of **Automatically select the certificate store based on the type of certificate**.

The wizard indicates that "You have successfully completed the Certificate Import wizard."

f Click **Finish**.

A **Security Warning** indicates that "You are about to install a certificate from a certification authority claiming to represent: CMA Self-Signed Certificate" and asking you "Do you want to install this certificate?"

g Click **Yes**.

The wizard indicates that "You have successfully completed the Certificate Import wizard."

h Click **Finish**.

A **Security Warning** indicates that "You are about to install a certificate from a certification authority claiming to represent: CMA" and asking you "Do you want to install this certificate?"

i Click **Yes**.

The Polycom CMA system log in page appears. The next time you access the Polycom CMA system , the **Security Alert** indicates "The security certificate is from a trusted certifying authority."

Change the Polycom CMA System User Interface Timeout

By default the Polycom CMA system user interface times out after a 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer or to turn it off.

To change the Polycom CMA system user interface timeout

1 Go to **Admin > Management and Security Settings > Security Settings**.

2 In the **CMA User Interface Timeout** section of the **Security Settings** page:

a To disable the **CMA User Interface Timeout**, by change the drop-down menu to **OFF**.

b To change the **CMA User Interface Timeout** value,

3 Click **Update**.

Change the Default User Access to the Polycom CMA System

By default when local users are added to the Polycom CMA system, they are assigned the **Scheduler** role, but enterprise users are not assigned a default role. Use this procedure to change whether or not enterprise users are assigned the **Scheduler** role by default.

To change the default access to the Polycom CMA system

1. Go to **Admin > Management and Security Settings > Security Settings**.
2. To allow default access, change the **CMA Access via default profile allowed** value to **ON**.
3. To change the message unauthorized users see, edit the **Message to be displayed to unauthorized users**.
4. Click **Update**.

Automatic Registration Server Addressing

You can configure the Polycom CMA system to send registration server addressing information for the gatekeeper and/or global directory server (GDS) when the endpoint is registered to the Polycom CMA system.

This automatic registration service only works for endpoints that register with the gatekeeper or GDS (or are manually added to the Polycom CMA system) after the Automatic Registration Service setting is enabled.

So if the Automatic Registration Service setting is enabled and an endpoint registers with the gatekeeper, the gatekeeper addressing information is sent to the endpoint. If the Automatic Registration Service setting is enabled and an endpoint registers with the GDS, the GDS addressing information is sent to the endpoint. If the Automatic Registration Service setting is enabled and an endpoint is added manually to the Polycom CMA system, both the gatekeeper and GDS addressing information is sent to the endpoint.

If automatic discovery and configuration is not successful, you can manually add endpoints.

Notes

- Automatic discovery works only for endpoints that register with the gatekeeper or Global Directory Server after the Automatic Discovery setting is enabled; it does not automatically discover existing endpoints.
- The Polycom CMA system only supports automatic discovery for V-Series, VSX-Series, and Polycom HDX-Series devices operating in traditional mode.

To enable automatic discovery of endpoints

1 Go to **Admin > Management and Security Settings > Endpoint Management Settings**.

2 In the **Automatic Endpoint Discovery** section of the **Endpoint Management Settings** page, select **Discover Endpoints** and click **Update**.

After you have changed this setting, all endpoints you add are automatically provisioned.

Set Common Passwords for Endpoints

The **Common Password** feature allows you to manage endpoints that have the same global administrative password. However, it cannot reset the administrative password on endpoints.

If you use the **Common Password** feature, access to password-protected data within endpoints is granted if the specified common password matches the endpoints' **Administrator Password**.

To set common passwords for endpoints

1 Go to **Admin > Management and Security Settings > Endpoint Management Settings**.

2 In the **Common Password** section of the **Endpoint Management Settings** page, select **Use a Common Password**.

3 Enter the common password in the **Password** and **Verify Password** fields and click **Update**.

Note

Leave these three settings blank if your Polycom endpoints require individual passwords or do not have passwords. To configure a global administrative password for all Polycom endpoints, use scheduled provisioning.

In a redundant configuration, repeat steps 1 through 3 on the redundant server.

29

Dial Plan Setup

This chapter describes how to edit the default Polycom CMA system Dial Plan settings to support your company's site topology. It includes these topics:

Site Operations

Site operations include:

View the Graphical Site Topology

To view the graphical site topology

>> Go to **Admin > Dial Plan and Sites > Site Topology**.

The **Site Toplogy** page appears. It graphically displays the sites and site links defined to the Polycom CMA system. To view information about a site or site link, mouse over the item of interest and the system displays information about the item.

View the Sites List

To view the Sites list

>> Go to **Admin > Dial Plan and Sites > Sites**.

The **Sites** list appears. It includes this information:

Column	Description
Name	The physical location of the site
Description	Description of the site
Country Code	The country code for the site
Area Code	The area code for the site

Add a Site

To add a site

1. Go to **Admin > Dial Plan and Sites > Sites**.
2. In the **Sites** list, click **Add Site**.
3. In the **Add Site** dialog box, enter a **Site Name** and **Description** for the site.
4. Complete the **General Info**, **Site Routing**, **Site Subnet**, and if applicable **ISDN Number Assignment,** sections of the **Add Site** dialog box.
5. Click **OK**.

   The new site is added to the system and the **Edit Site Provisioning** dialog box appears. These are the site-based parameters that the Polycom CMA system automatically provisions to endpoint systems operating in dynamic management mode.
6. As needed, edit the default site provisioning details and click **Apply**.

Note

Not all of the site provisioning parameters apply to all endpoint systems being provisioned. If an endpoint system does not have a corresponding parameter, it ignores the parameter.

Field	For the endpoint systems at the site being provisioned...
Date and Time Settings	
Country	Specifies the country code for their location.
Date Format	Specifies the date display format.
Auto Adjust for Daylight Saving Time	Specifies whether or not to adjust the endpoint's system clock for daylight savings time.
Time Format	Specifies the time display format.
Time Server	Specifies whether to connect to a time server for automatic system time settings. Select **Auto** to require that the video endpoint system synchronize with an external time server that is identified by a network domain controller. Because it is identified by a network domain controller, you do not need to enter the IP address of the time server. Select **Manual** to require that the video endpoint system synchronize with an external time server that may not be identified by a network domain controller. In this case, you must also enter the IP address of the time server in the **Time Server Address** field. If **Time Server** is set to **Off**, or if the **Time Server** is set to **Manual** or **Auto** but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.
Time Server Address	Specifies the address of the time server when **Time Server** is set to **Manual**.
Timezone	Specifies the time difference between GMT (Greenwich Mean Time) and the endpoint system's location.
Firewall Settings	
Use Fixed Ports	Specifies whether to define the TCP and UDP ports. • If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. • If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. **Note** You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic.
Start TCP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specifiy. **Note** You must also open the firewall's TCP port 1720 to allow H.323 traffic.
Start UDP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specifiy.
Enable H.460 Firewall Traversal	Allows the endpoint system to use H.460-based firewall traversal. For more information, see the *Administrator's Guide for Polycom HDX Systems*.

Field	For the endpoint systems at the site being provisioned...
NAT Configuration	Specifies whether the endpoint systems should determine the NAT Public WAN Address automatically. • If the endpoint systems are behind a NAT that allows HTTP traffic, select **Auto**. • If the endpoint systems are behind a NAT that does not allow HTTP traffic, select **Manual**. Then specify a **NAT Public (WAN) Address**. • If the endpoint systems are not behind a NAT or are connected to the IP network through a virtual private network (VPN), select **Off**.
NAT Public (WAN) Address	When **NAT Configuration** is set to **Manual**, specifies the address that callers from outside the LAN should use to call the endpoint systems.
NAT is H.323 Compatible	Specifies that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.
Address Displayed in Global Directory	Specifies whether to include the endpoint system's information in the global directory • Select **Private** to exclude the endpoint from the global directory • Select **Public** to include the endpoint in the global directoyr
H323 Settings	
Enable IP H.323	Specifies whether to enable IP H.323 calls.
Use Gatekeeper	When IP H.323 is enabled, specifies whether the endpoint systems will use the Polycom CMA system as its gatekeeper or another gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **This Server** — The endpoint systems will use the Polycom CMA system as their gatekeeper. • **Specify** — The endpoint systems will use another system as their gatekeeper.
Gatekeeper IP Address	When **Use Gatekeeper** is set to **Specify**, enter the gatekeeper IP address in this field.
Use Gatekeeper for Multipoint Calls	Specify whether multipoint calls use the endpoint system's internal multipoint capability or the Polycom MCU's Conference on Demand feature. This feature is available only if the system is registered with a PathNavigator or Polycom CMA system gatekeeper.
Provisioning Settings	
Provisioning Polling Interval (minutes)	Specifies the frequency at which the endpoint systems poll the Polycom CMA system for new provisioning information. By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the Polycom CMA system for new provisioning information.
Softupdate Polling Interval (minutes)	Specifies the frequency at which the endpoint systems poll the Polycom CMA system for a new softupdate package. By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced. When the value of this interval is set to 0, the endpoint systems do not poll the Polycom CMA system for a new softupdate package.

Field	For the endpoint systems at the site being provisioned...
Quality of Service Settings	
Video Type of Service Value	Specifies the IP Precedence or Diffserv value for video packets.
Audio Type of Service Value	Specifies the IP Precedence or Diffserv value for audio packets.
FECC Type of Service Value	Specifies the IP Precedence or Diffserv value for Far End Camera Control packets.
Type of Service Field	Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedenc**e — Represents the priority of IP packets sent to the system. The value can be between 0 and 5. • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.
Maximum Transmission Unit Size (bytes)	Specifies the Maximum Transmission Unit (MTU) size used in IP calls. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small; increase the MTU.
Enable PVEC	Allows the endpoint system to use PVEC (Polycom Video Error Concealment) if packet loss occurs. PVEC delivers smooth, clear video over IP networks by concealing the deteriorating effects of packet loss
Enable RSVP	Allows the endpoint system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.
Enable Dynamic Bandwidth	Specifies whether to let the endpoint system automatically find the optimum line speed for a call.
Maximum Transmit Bandwidth (Kbps)	Specifies the maximum transmission line speed.
Maximum Receive Bandwidth (Kbps)	Specifies the maximum reception line speed.
Security Settings	
Use Room Password for Remote Access	Specifies whether the local endpoint system password and remote access password are the same.
Room Password	Enter or change the local endpoint system password here. When the local password is set, you must enter it to configure the system Admin Settings using the remote control. The local password must not contain spaces.
Remote Access Password	For endpoint systems, enter or change the remote access password here. When the remote access password is set, you must enter it to upgrade the software or manage the endpoint systems from a computer. The remote access password cannot include spaces.

Field	For the endpoint systems at the site being provisioned...
Meeting Password	Specifies the password users must supply to join multipoint calls on this endpoint system if the call uses the internal multipoint option, rather than a bridge. This field can also be used to store a password required by another endpoint system that this system calls. If a password is stored in this field, you do not need to enter it at the time of the call; the endpoint system supplies it to the system that requires it. The meeting password cannot include spaces.
Enable Secure Mode	Specifies whether to operate in secure mode (also known as security mode), which uses TLS, HTTPS, AES, digital signatures, and other security protocols, algorithms, and mechanisms. These protocols encrypt management communication over IP, preventing access by unauthorized users. When devices at a site are provisioned to operate in secure mode, the Polycom CMA system can only perform the dynamic management operations of automatic provisioning, automatic softupdate, and directory and presence services for the devices. The Polycom CMA system cannot perform monitoring or control operations for the devices. For more information, see the *Administrator's Guide for Polycom HDX Systems*.
Enable Encryption	Specifies how to encrypt calls with other sites that support AES encryption. • **Off**—No encryption is used. • **When Available**—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don't support it. • **Required for Video Calls Only**—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. • **Required for All Calls**—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must. support AES Encryption to participate in the call.
Enable Web Access	Specifies whether to allow remote access to the endpoint system by the web. **Note** The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the **Web Access Port** setting to disable the port.
Enable Telnet Access	Specifies whether to allow remote access to the system by Telnet. **Note** The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the **Web Access Port** setting to disable the port.
Enable SNMP Access	Specifies whether to allow remote access to the system by SNMP. **Note** The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the **Web Access Port** setting to disable the port.

Field	For the endpoint systems at the site being provisioned...
Web Access Port	Specifies the port to use when accessing the endpoint system's web interface. If you change this from the default (port 80), specify a port number of 1025 or higher, and make sure the port is not already in use. You will need to include the port number with the IP address when you use the Polycom HDX web interface to access the system. This makes unauthorized access more difficult. **Note** The system restarts if you change the web access port.
Allow Video Display On Web	Specifies whether to allow viewing of the room where the endpoint system is located, or video of calls in which the endpoint system participates, using the endpoint system's web interface. **Note** This feature activates both near site and far site video displays in Web Director.
CMA Desktop Settings	
Heartbeat Posting Interval (minutes)	Specifies the frequency at which the endpoint systems poll the Polycom CMA system for a heartbeat.
In Call Stats Posting Interval (minutes)	Specifies the frequency at which the endpoint systems poll the Polycom CMA system for in call statistics.

Edit Site Settings

Note
Changing network topology may affect the accuracy of reports based on this information. To retain historical data for the current network topology, generate reports before making changes.

To edit settings for a site

1. Go to **Admin > Dial Plan and Sites > Sites**.
2. In the **Sites** list, select the site of interest and click **Edit Site**.
3. Edit the **General Info**, **Site Routing**, **Site Subnet**, and if applicable **ISDN Number Assignment,** sections of the **Edit Site** dialog box.
4. Click **OK**.

   The **Sites** list reappears.

Delete a Site

Note
Devices that belonged to a deleted site are automatically reassigned to support Internet and VPN calls.

To delete a site

1. Go to **Admin > Dial Plan and Sites > Sites** or **Admin > Dial Plan and Sites > Site Topology**.
2. In the **Sites** list or **Site Topology** page, select the site of interest and click **Delete Site**.
3. Click **Yes** to confirm the deletion.

Site Link Operations

When you add a site link, you enter the starting and ending sites of the link and the maximum bandwidth and bit rates available for video calls that use the link.

Note
The bit rate can be set at the network level, the device level, and the conference level. If there is a discrepancy between these bit rate settings, the system implements the lowest bit rate setting. The only exception, is that the bit rate in the RMX profile takes precedence over the bit rate in the conference settings.

When you define site topology, define the direct links first so you can use them to define multisite links.

You create multisite links by defining a network path that consists of multiple direct links. You can define only the most cost-efficient path or create multiple paths and use least-cost routing tables.

Note
Links are bidirectional. After you have created a link from Site A to Site B, you automatically have a link from Site B to Site A, although the link appears as unidirectional.

Field	Description
Name	Name (ASCII only[a]) of the inter-site link
Description	Description (ASCII only[a]) of the inter-site link

Field	Description
From Site	Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.
To Site	Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet/VPN option.
Link Type	Specifies a direct link between two physical sites or a multisite link, for which a path of links is defined
Total Bandwidth (kbps)	The maximum available bandwidth for audio and video calls, which you set at the gateway or router. Only applies to direct links. The bandwidth on multisite links is the lowest respective value from the list of direct links.
Call Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call. Only applies to direct links. The bit rate on multisite links is the lowest value from the list of direct links.

a. For more information, see "Field Input Requirements" on page 6.

Site-link operations include:

- View the Site Links List
- Add a Site Link
- Edit a Site Link
- Delete a Site Link

View the Site Links List

To view the Site Links list

>> Go to **Admin > Dial Plan and Sites > Site-Links**.

The **Site-Links** list appears.

Column	Description
Name	Name of the link
Description	Description of the link
From Site	First site reached in the call route
To Site	Final site reached through this call link
Link Type	Indicates a direct link from one site to another or a multisite link, which may use a path through several different sites and the Internet

Column	Description
Max Bandwidth	The maximum available bandwidth for audio and video calls, which you set at the gateway or router. Only applies to direct links. The bandwidth on multisite links is the lowest respective value from the list of direct links.
Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call. Only applies to direct links. The bit rate on multisite links is the lowest value from the list of direct links.

Add a Site Link

To add a site link

1. Go to **Admin > Dial Plan and Sites > Site-Links**.
2. In the **Site-Links** list, click **Add Site-Link**.
3. In the **Add Site-Link** dialog box, enter a **Name** and **Description** for the link and select the starting (**From Site**) and ending (**To Site**) sites.
4. To add a direct site links, enter the **Bandwidth** and **Max Bit Rate** and click **Save**.
5. To add a multisite link:
   a. Click **MultiSite**.
   b. Select the first site from the **Available Direct Links** column and move it to the **Selected Direct Links** column.
   c. Select the second site from the **Available Direct Links** column and move it to the **Selected Direct Links** column.

Note
If you receive a **Select Destination Place** dialog box, click **OK** and continue.

   d. Add additional site links as required.
   e. Click **Save**.

   The new link appears on the **List of site Links** page.

Edit a Site Link

You may need to edit site link when network changes are made.

If you make a bandwidth change, the current load is not affected; however, the bandwidth available for future conferences may be affected.

To edit a site link

1. Go to **Admin > Dial Plan and Sites > Site-Links**.
2. In the **Site-Links** list, select the link of interest and click **Edit Site-Link**.
3. In the **Edit Site-Link** dialog box, edit the **Name**, **Description, Bandwidth** or **Max Bit Rate**.
4. Click **Save**.

Delete a Site Link

You can remove site links from the CMA system.

> **Note**
> Avoid removing a link on which a scheduled conference depends.

To delete a site link

1. Go to **Admin > Dial Plan and Sites > Site-Links**.
2. In the **Site-Links** list, select the site link of interest and click **Delete Site-Link**.
3. Click **Yes** to confirm the deletion.

Dial Plan Service Operations

Dial plan services are special features that video endpoint system users can invoke by dialing the prefix assigned in the Polycom CMA system to that service.

The Polycom CMA system has two default dial plan services: Conference on Demand and Simplified Dialing, which are described in the sections that follow. These services can be edited and disabled, but not deleted.

You can also add other gateway or If a service does not appear automatically when a device registers with the Polycom CMA system, you can define the service manually so that it is available for video endpoint system users. In addition, you can add services for certain third-party MCU services.

Conference on Demand

With Conference on Demand, video endpoint system users can start an unscheduled multipoint conference from their endpoint rather than requesting this service from an administrator.

The initiating endpoint uses the capabilities made available through the MCU. When Conference on Demand is enabled on the endpoint, the Polycom CMA system sends the call directly to the MCU.

Note

Conference on Demand is only available on Polycom RMX 2000 and Polycom MGC MCUs. It is not available on Polycom RMX 1000 MCUs.

The following table provides details on how the Conference on Demand service is configured.

Field	Description
General Info	
Service Type	Conference on Demand (read only)
Enable	Indicates whether or not the service is enabled
Available for New Groups	Indicates whether or not the service is available for new user groups
Description	Description (ASCII only[a]) of the service. By default for this service, Conference on Demand
Service Prefix	The prefix (ASCII only[a]) for the service. By default for this service: con
Conference on Demand—MCU Properties	
Login ID	User login (ASCII only[a]) for the MCU hosting the conference. This user account must be authorized to create new conferences.
Password	Password (ASCII only[a]) for the user login. Each time you modify the password for the MCU, you must also modify it in this page.
H.323 Network Service	The corresponding service created on the MCU to implement this Polycom CMA system service. Set on the MCU (ASCII only[a]).

Field	Description
Default Conference Properties	
MGC: Video Session	Indicates what users see. Set to **Continuous Presence** for this service. **Notes** • MGC only. For the RMX 2000 MCU, the profile determines this setting. • Select **Transcoding** to support IP and ISDN calls.
MGC: Bit rate (Kbps)	Default bit rate for calls. **Notes** • MGC only. The RMX 2000 MCU bit rate is dictated by the RMX profile. • The video endpoint system that starts the Conference on Demand call may use a higher or lower bit rate than is specified in this page.
RMX: Profile Name	The name of the RMX profile that has the conference settings for the conference.

a. For more information, see "Field Input Requirements" on page 6.

Simplified Dialing

Simplified dialing is a service that allows video endpoint system users to access gateway services by dialing 9, and then the phone number or other dialing string. Simplified dialing is enabled by default.

To use simplified dialing, the following settings are also required:

- Sites must specify the country code, city and area code, and number of digits in the subscriber line.
- The gateway must be registered with the Polycom CMA system and display in the **List of Devices** page.
- Gateway services must be defined.
- The LCR table must be defined.

Field	Description
Service Type	Name of the service (read only)
Enable	Indicates whether this service is enabled
Available for New Groups	The service is available for new user groups
Description	Description of the service
Service Prefix	The prefix for this service: 9.

Gateway Service

These services are provided by a gateway to endpoints. For example, gateways usually have distinct services for each speed they support (128 Kbps, 384 Kbps, 512 Kbps, and so on) and a service for audio-only calls.

Gateway services tell the Polycom CMA system how to route the call during conversion between IP and ISDN.

Note

Gateway and MCU services must be defined in both the Polycom CMA system and the MCU platform. They must be defined exactly the same in both locations. If you enter this information manually, be sure to type it exactly as it is entered in the MGC or RMX 2000 system.

You can simplify entry of services by making sure that the MCUs and gateways on your video conferencing network are set to register with the gatekeeper in the Polycom CMA system. This setting assures the information appears automatically in the **List of Services** page.

You must define a gateway service for each bit rate available. These services should appear automatically in the list when the gateway registers with the Polycom CMA system. If gateway services do not appear, you can enter them manually. If the **List of Services** page does not include gateway services, alternate routing and least-cost routing are disabled. For details, see the following table.

Field	Description
Service Type	Type of service
Enable	Indicates whether this service is enabled
Available for New Groups	The service is available to new user groups
Description	Description of the service
Service Prefix	The prefix for this service. Must be a registered E.164 alias for the corresponding gateway in the **Devices** page for **Directory Setup**.
For use in simplified dialing	
Device Capability	Specifies the type of connection the device can handle. Select all that apply. Options are: • **H.320.** Supports video and voice using the ITU H.320 standard. • **Voice.** Supports voice over the PSTN network. • **Other.** Supports a protocol other than H.320 or voice, such as H.321 or video over ATM.

Field	Description
Bit Rate (Kbps)	The maximum rate at which the calls can connect. **Note** If you select **Unknown**, this service cannot support simplified dialing.
Insert between prefix and first number	Specifies the character to insert in the dial string between the prefix and the first number. For example, if you specify * as the character, the sequence the user enters would be: 77*2125551212
Insert between phone number	Specifies the character to insert in the dial string between phone numbers. For example, if you specify # as the character to separate numbers, the sequence the user enters would be: 77*5551212#5651213
Append after full dial string	Specifies the character to append after the full dial string. To process the call, certain gateways require a symbol be appended after the final dialing number. For example, if you specify ** as the characters to append after the final dialing number, the sequence the user enters would be: 77*5551212#5651213#2223232** **Warning:** The Polycom CMA system does not recognize dial strings that require termination after the ISDN number and have an extension after the terminated ISDN. For example, the CMA system does not recognize the following dial string: 165024710000**3452

MCU Service

These services allow devices to use specific MCU features and settings when making a call. For example, an MCU can define a service for a multipoint video call with continuous presence at 384 Kbps and another service for video switching at 256 Kbps.

MCU services and their associated prefixes are defined at the MCU. For MGC or RMX 2000 devices, the MCU services should appear automatically in the **List of Services** page when the MCU registers with the Polycom CMA system. Because third-party MCUs may not automatically register, you must enter them manually in the Polycom CMA system.

Use MCU services to dial the IP gateway segment that translates between IP and ISDN, in conference calls with two or more participants, or continuous presence.

Field Name	Description
Service Type	Type of service.
Enable	Indicates whether this service is enabled or not.
Available for New Groups	The service is available for new user groups.
Description	Description of the service. To identify it easily in the **List of Services** page, include the prefix and the MCU feature (for example, 384 K video switching).
Service Prefix	The prefix for this service, which must be a E.164 alias that is registered for the MCU on the Device page.

Services operations include:

- View the Services List
- Add a Service
- Edit a Service
- Delete a Service

View the Services List

This page shows the services that have been defined in your dial plan. These services are available when you place unscheduled calls.

Note

E.164 aliases appear in this list as follows:

- For MGC and RMX 2000 devices, they appear as gateway services.
- For a device's H.323 services, they (including the alias prefix) appear as MCU services. Gateway service prefixes are the E.164 aliases of the MCU's gateway session profiles.

To view the Services list

>> Go to **Admin > Dial Plan > Services**.

The **Services** list appears.

Column	Description
Prefix	Prefix of the service.
Type	The type of service. Available types include System, Gateway, and MCU.

Column	Description
Description	Description of the service. **Tip:** When completed automatically, the description reflects the value entered in the MGC or RMX 2000 manager.
Enabled	By default, services are enabled. To disable them, clear the **Enabled** check box.

Add a Service

If a gateway or MCU service does not appear automatically when the device registers with the Polycom CMA system, you can define the service manually so that it is available for use in unscheduled calls. In addition, you can add services for certain third-party MCU services.

To add a service

1. Go to **Admin > Dial Plan > Services**.
2. In the **Services** list, click **Add Service**.
3. Complete the **General Info**, and if applicable **Simplified Dialing** or **Conference on Demand,** sections of the **Add Service** dialog box.
4. Click **OK**.

   The new service is added to the system.

Edit a Service

You can make changes to a service.

> **Note**
> Be sure that the information you enter in the Polycom CMA system matches the information entered in the MCU.

To edit a service

1. Go to **Admin > Dial Plan > Services**.
2. In the **Services** list, select the service of interest and click **Edit Service**.
3. As required, edit the **General Info**, and if applicable **Simplified Dialing** or **Conference on Demand,** sections of the **Edit Service** dialog box.
4. Click **OK**.

Delete a Service

You can delete a gateway or MCU service from the Polycom CMA system. You cannot delete the **Conference on Demand** or **Simplified Dialing** service.

To delete a service

1. Go to **Admin > Dial Plan > Services**.
2. In the **Services** list, select the service of interest and click **Delete Service**.
3. Click **Yes** to confirm the deletion.

Dial Rule Operations

Dial rules describe how the Polycom CMA system gatekeeper should resolve addresses in an incoming dial string to route a 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. However, you can assign a priority to each dial rule. When the Polycom CMA system gatekeeper receives a call request and associated dial string, it reviews the dial rules in order of priority. The first matched (highest priority) dial rule is executed.

Field	Description
General Info	
Name	Name (ASCII only[a]) of the dial rule.
Description	Description (ASCII only[a]) of the dial rule, which can be up to 256 characters long.
Priority	Priority number of the dial rule, which determines which rule the Polycom CMA system uses first. More than one dial rule may have the same priority. In that case, rules with the same priority are applied in random order.
Enabled	Select the check box to enable the rule.
Pattern Type	Specifies the type of pattern to be matched. Available patterns include: • Local Directory Services • DNS Name • IP Address • Prefix • Prefix Range

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Applicable Site	Site to which this pattern applies. You can select a specific site or all sites. This field is not available when the **Pattern Type** is **Local Directory Services**.
Routing Action > Dial String Manipulation	
IP Address Pattern Data	Specifies the criteria (ASCII only[a]) to use to match the pattern type and additional changes to make when routing the call. This field is available when the **Pattern Type** is **DNS Name**, **IP Address**, or **Prefix**. This field is not available when the **Pattern Type** is **Local Directory Services** or **Prefix Range**.
Start Value	The starting number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type.
End Value	The ending number to use as a prefix, which displays only for rules with the **Prefix Range** pattern type
# Characters to remove	Number of digits to remove (from the start or from the end) of the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Prefix to add	Prefix to add to the dialed string This field is available when the **Pattern Type** is **Local Directory Services**, **Prefix**, and **Prefix Range**. This field is not available when the **Pattern Type** is **DNS Name** or **IP Address**.
Routing Action > Action to perform	
Action	Specifies what action to take for calls that match the pattern type and criteria. Action to perform when the pattern is matched. Depending on the **Pattern Type**, options may include: • Route • Block • Route within region • Route out of region • Route to a gateway with LCR applied • Route to a gateway service • Route to a list of gateway services • Route to a trusted neighbor

Field	Description
Trusted Neighbors	
Available Region	When the action is **Route to a trusted neighbor**, select the region to which you want to route.
Gateway Services	
Selected Gateway Services (prioritized)	When the action is **Route to a gateway service**, this field lists the selected gateway services. You can define multiple gateway services for a rule. The first in the list is the default gateway service. Others are used in priority order when the primary gateway service is not available.

a. For more information, see "Field Input Requirements" on page 6.

Default Dial Rules

The Polycom CMA system has three default dial rules. With these defaults, the system can route most calls except those requiring an external DNS lookup.

- Internal IP - This dial rule allows the system to identify the incoming dial string as an IP addresses and routes the call out of the region. By default, this dial rule applies to all sites.
- Alias - This dial rule allows the system to identify the incoming dial string as belonging to the local directory and routes the call to the local device or service, as required.
- DNS Name - This dial rule allows the system to identify the incoming dial string as a DNS name and block the call.

Note

Do not delete the default dial rules or the CMA system will not be able to route calls correctly. You can disable a dial rule by editing it and clearing the **Enabled** check box for the rule.

Parts of a Dial Rule

A dial rule consists of a pattern type paired with a routing action. When the dialed string uses a pattern that matches the pattern type, the associated rule is applied.

Pattern Types

A pattern type tells the Polycom CMA system how to find a match for the dial string. The following table shows the available pattern types.

Pattern Type	Description
Local Directory Services	Search the **List of Devices** and **List of Services**. Includes aliases, which are searched before the service prefix.
DNS Name	Look up a DNS Name
IP Address	Look for an IP addresses in the IPV4 format
Prefix	Look for a prefix specified in the dial rule
Prefix Range	Look for a prefix within the range of prefixes specified in the dial rule

Routing Actions

A routing action informs the Polycom CMA system what to do based on the dial rule's associated pattern type. The following table shows the available routing actions.

Routing Action	Pattern Type	Description
Route	All	Allow the call to pass
Block	All	Block the call
Route within region	IP Address	Route to any IP address inside the region
Route out of region	IP Address	Route to any IP address outside the region **Note** The originating site's Internet access rules still apply.
Route to a gateway with LCR	Prefix and Prefix Range	Remove the prefix specified in the dial rule and route the remaining dial string to a gateway service, which has the specified LCR table

Routing Action	Pattern Type	Description
Route to a gateway service	Prefix and Prefix Range	Remove the prefix specified in the dial rule and route the remaining dial string to the specified gateway service
Route to a list of gateway services	Prefix and Prefix Range	Modify the dial string specified in the dial rule and route the remaining dial string to the specified gateway service.
Route to a trusted neighbor	Prefix and Prefix Range	Modify the dial string as specified in the dial rule and ask the specified neighboring gatekeeper to route the modified dial string. If the neighboring gatekeeper agrees, route the call. **Note** The neighboring gatekeeper must be configured as a region in the CMA system.

Examples of Custom Dial Rules

You use custom dial rules to perform these tasks:

- **Block calls.** For example, you can block all calls to 900 numbers, which usually charge a per-minute fee. Create a dial rule with these settings:
  - Pattern type: Prefix
  - Prefix to match: 900
  - Routing action: Block
- **Route to a neighboring gatekeeper.** If you have entered information about neighboring gatekeepers in the **List of Regions** page, you can create a rule to route calls to another gatekeeper. Create a dial rule with these settings:
  - Pattern type: Prefix Range
  - Prefixes to match: Specify the range.
  - Routing action: Select **Route to a trusted neighbor** and the region for the neighboring gatekeeper to which you want to route calls.
- **IP-specific routing.** You can specify which calls may connect, according to the IP address. For example, you could allow calls from San Jose to Atlanta, but not from San Jose to Pleasanton.

Dial Rule operations include:

- View the Dial Rules List
- Add a Dial Rule
- Enable or Disable Dialing Rules
- Edit a Dial Rule

View the Dial Rules List

To view the Dial Rules list

>> Go to **Admin > Dial Plan > Dial Rules**.

The **Dial Rules** list appears.

Column	Description
Name	The name of the dial rule
Pattern Type	The pattern type in use for this rule. Options are: • Local Directory Services • DNS Name • IP Address • Prefix • Prefix Range For more information, see "Parts of a Dial Rule" on page 310.
Pattern Data	Additional criteria that must be met to apply this rule
Routing Action	The routing action used by this rule. Options are: • Route • Block • Route within region • Route out of region • Route to a GW with LCR applied • Route to a GW service • Route to a list of GW services • Route to a trusted neighbor **Note** Not all actions are available for all pattern types.
Site	The sites for which this rule is used. May be all sites or a specific site
Priority	The priority assigned this rule
Enabled	Indicates whether or not the dial rule is enabled

Add a Dial Rule

To add a dial rule

1. Go to **Admin > Dial Plan > Dial Rules**.
2. In the **Dial Rules** list, click **Add Dialing Rule**.
3. Complete the **General Info**, **Routing Action**, **Trusted Neighbors, and Gateway Services** sections of the **Add Dialing Rule** dialog box.
4. Click **OK**.

   The new dial rule is added to the system.

Enable or Disable Dialing Rules

You can enable or disable dial rules.

> **Note**
> Use caution when changing the default dial rules, which enable basic operations in the CMA system.

To enable or disable a dialing rule

1. Go to **Admin > Dial Plan > Dial Rules**.
2. In the **Dial Rules** list, select the dial rule of interest and click **Edit Dialing Rule**.
3. On the **Dial Rules - General Information** page, check or uncheck the **Enabled** check box.
4. Click **OK**.

Edit a Dial Rule

To edit a dial rule

1. Go to **Admin > Dial Plan > Dial Rules**.
2. In the **Dial Rules** list, select the dial rule of interest and click **Edit Dial Rule**.
3. In the **Edit Dial Rule** dialog box, make the required changes.
4. When you are finished, click **OK**.

Least-Cost Routing Operations

Least-cost routing (LCR) allows the Polycom CMA system to route ISDN or POTS calls made on paths that incur the lowest expense. You can route calls from one site through a gateway in another site by referencing LCR tables.

Least-cost routing is useful when sites already have a high-bandwidth connection between them.

Least-cost routing works with the Polycom CMA system's other routing features.

Setting up least-cost routing requires you to:

- Determine the LCR information to enter in the Polycom CMA system.
- Create LCR tables.
- In the device record for MCUs:
  - Define an H.320 service and select the LCR table to use.
  - Define a gateway service and select the H.320 service associated with the LCR table.

Note
Make sure the LCR tables you define match the network setup.

You cannot use least-cost routing when:

- The route cannot be identified.
- The required resources are unavailable.
- Bandwidth limitations exist on the WAN.

How Least-Cost Routing Works

Each LCR table defines dial strings, which include the country code, area code, prefix, and a weighted cost for commonly made calls. You usually create one LCR table per site.

The following table is an example of an LCR table.

Country Code	Area Code	Prefix	Weighted Cost
1	408	565	0
1	408		0
1	650		0
1	415		5

The Polycom CMA system compares the dial string for a call to the dial strings in LCR tables. The dial string can match at the country code, area code, or prefix level. The CMA system reads the "# of digits to strip" field to determine how many digits to remove.

Note

For areas of the United States that do not require you dial an access code before the area code, exclude this number when you define the number of digits to strip.

Before determining the final call routing, the Polycom CMA system considers cost (through LCR tables), bandwidth resources (through site topology and device group policies), and gateway availability.

Example of Least-Cost Routing

Company ABC has three sites: Site A in San Jose, CA, Site B in Monterey, CA, and Site C in Washington, D.C. All sites have gateways.

LCR Tables for Three Sites

The LCR tables included area codes that are used frequently in each site and considered that calls are made frequently from Site C to Southern California.

The following table lists area codes for the San Francisco Bay Area and Southern California. The prefix 755 for the 408 area code applies for all numbers in Site A.

Area Code	Prefix	Weighted Cost
408	755	0
408		0
650		0
510		0
925		0
415		5
831		5
213		10
310		10
714		10
		20

The following table lists area codes for Washington, D.C., Eastern Maryland, and Northeastern Virginia.

Area Code	Prefix	Weighted Cost
202	238	0
202		0
240		0
301		0
741		0
703		0
410		5
443		5
540		5
804		10
		20

The following table lists area codes for San Jose, Monterrey, and Southern California.

Area Code	Prefix	Weighted Cost
831	477	0
831		0
408		5
213		10
310		10
714		10
		20

Call Scenario One

Site C can call San Jose using ISDN through one of two routes:

- Through the Site C gateway to the local phone system, making a long distance connection, at a higher cost per minute.
- From Site C through the direct inter-site link to Site A and out its gateway, at a lower cost per minute.

Note
If you dial an area code that is not in an LCR table, the call goes through the gateway from which the call originates.

Call Scenario Two

Calls are frequently made from Site C to Los Angeles. The area codes for some parts of Southern California are included in the LCR tables for Sites A and B, because it is less expensive to make an intrastate long distance call within California than an interstate long distance call from Washington, D.C. to Los Angeles.

By including Southern California area codes in LCR tables for San Jose and Monterey, if the bandwidth for the San Jose gateway is saturated, the call from Site C can be routed through the Monterey gateway. The priority is to call from Site A or Site B, because the LCR tables share a relative cost to dial the area codes for Los Angeles.

Determining Area Codes

It is recommended you enter area codes for:

- The area in which the site is located.
- The area surrounding the site.
- Frequently called numbers.

Note
You should also include special rate plans for intrastate calling.

Determining Country Codes

If you make international calls and you determine that calls to a certain country are less expensive from a particular gateway, enter the dial string for this country in the LCR table for the selected gateway.

Determining the Weighted Cost

When you enter call strings in an LCR table, associate a weighted cost with each one. You can base the cost on a monetary value or ratio that compares costs between several locations. The weighted cost determines which call string is most cost-effective to use.

You can calculate costs for the following types of calls:

- Local
- Local toll
- Intrastate
- Interstate
- International long distance

Field	Description
Name	Name (ASCII only[a]) for the LCR table.
Description	(Optional) (ASCII only[a])
Country	Country code for the location to which this call is made.
City Code	City or area code for the location to which this call is made.
Prefix	The prefix is the first three numbers in a 7-digit dial string.
# Digits to Strip	The number of digits to strip before dialing.
Cost	Weighted cost for each call to the selected area or city code.

a. For more information, see "Field Input Requirements" on page 6.

LCR operations include:

- View the Least Cost Routing Tables List
- Add a Least Cost Routing Table
- Edit a Least Cost Routing Table
- Delete a Least Cost Routing Table

View the Least Cost Routing Tables List

Column	Description
Name	Name of the LCR table.
Description	Description of the LCR table.

To display the list of least cost routing tables

>> Go to **Admin > Dial Plan > LCR Tables**.

The **LCR Tables** list appears.

Add a Least Cost Routing Table

To add a LCR table

1. Go to **Admin > Dial Plan > LCR Tables**.
2. In the **LCR Tables** list, click **Add LCR**.
3. In the **Add LCR Tables** dialog box, enter the **Name**, **Description**, and **New Route** information required to create a new table.
4. Click **Add**.
5. Repeat step 3 and 4 for add additional routes to the table.
6. Click **OK**.

Edit a Least Cost Routing Table

To edit an LCR table

1. Go to **Admin > Dial Plan > LCR Tables**.
2. In the **LCR Tables** list, select the table of interest and click **Edit LCR**.
3. In the **Edit LCR** dialog box, edit the **Name**, **Description**, and **New Route** information as required.
4. Click **Save**.

   The changes you made apply to all MCUs associated with a gateway service that uses this LCR table.

Delete a Least Cost Routing Table

To delete an LCR table

1. Go to **Admin > Dial Plan > LCR Tables**.
2. In the **LCR Tables** list, select the table of interest and click **Delete LCR**.
3. Click **Delete** to confirm the deletion.

30

Remote Alert Setup Operations

This chapter describes how to configure the Polycom® Converged Management Application™ (CMA™) system to send alerts remotely to users via email for specific types of system and endpoint events. It includes these topics:

- Set Up Remote Alerts
- Edit a Remote Alert Profile
- Disable a Remote Alert Profile
- Delete a Remote Alert Profile
- Disable Polycom CMA System Remote Alerts

Set Up Remote Alerts

To set up remote alerts, you must complete the following tasks:

1. Set Up Polycom CMA System-generated Email Account.
2. Enable Polycom CMA System Remote Alerts.
3. Set Polycom CMA System Remote Alert Level Settings.
4. Set Endpoint Alert Level Settings.
5. Add a Remote Alert Profile.
6. Associate a Remote Alert Profile With a User.

Set Up Polycom CMA System-generated Email Account

To set the Polycom CMA system-generated email account

1 Go to **Admin > Server Settings > Email**.

2 On the **Email** page, enter the email account (ASCII only) from which the Polycom CMA system will send conference notification emails.

By default, the Polycom CMA system emails are addressed as `PanAlert@vtcmanager.com`.

3 Specify the IP address of the mail server from which the Polycom CMA system will send conference notification emails.

Notes

- Many E-mail servers will block or discard emails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid email address.
- Many E-mail servers will block or discard emails from un-trusted domains, in which case you may need to change the default Polycom CMA system email address to one in a trusted domain.

4 Click **Update**.

Enable Polycom CMA System Remote Alerts

To enable Polycom CMA system remote alerts

1 Go to **Admin > Server Settings > Remote Alert Setup**.

2 On the **Remote Alert Setup** page, select **Enable Remote Alerts**.

3 Set a **Remote Alert quiescent time**, which is the amount of time (in minutes) the system should wait after alerts have been detected but not cleared before starting the alert notification process, and if applicable, the remote alert notification process.

4 Click **Update**.

Set Polycom CMA System Remote Alert Level Settings

To set the Polycom CMA system remote alert level settings

1 Go to **Admin > Alert Settings > CMA Alert Level Settings**.

2 On the **CMA Alert Level Settings** page, change the **Alert Severity Level** for the different types of system events as required.

Alert Type	Description
Bridge Down	Indicates a Polycom MCU (RMX or MGC) has failed.
Database Connection Down	Indicates the connection to the database has been lost.
LDAP Connection Down	Indicates the connection to the LDAP server has been lost.
LDAP System Account Password Failure	Indicates the connection to the LDAP server could not be established because the account password was incorrect.
CMA Failover Occurred	In redundant Polycom CMA system configurations only. Indicates the system has failed over from one system server to the other.
License Capacity Threshold Exceeded	Indicates that the number of available seats defined by the installed license is within 5% of the total license capacity.
Bridge Time Discrepancy	Indicates there is a difference between the clock on the Polycom MCU (RMX or MGC) and the Polycom CMA system clock.
CMA Monitor Service Stopped	In redundant Polycom CMA system configurations only. Indicates that the Polycom CMA system redundancy monitoring service is not running.
Redundant Service Down	In redundant Polycom CMA system configurations only. Indicates that the connection or synchronization between the primary and secondary server has been lost.
Redundancy Conflict	In redundant Polycom CMA system configurations only. Indicates that both the primary and secondary system servers believe they are the active server.

3 Click **Update**.

Set Endpoint Alert Level Settings

To set the endpoint alert level settings

1 Go to **Admin > Alert Settings > Endpoint Alert Level Settings**.

2 On the **Endpoint Alert Level Settings** page, change the **Alert Severity Level** for the different types of endpoint events as required.

Alert Type	Description
Incorrect Password	Indicates the connection to the endpoint could not be established because the password was incorrect.
IP Conflict	Indicates the system has detected another device with the same IP as the endpoint and the discrepancy cannot resolved.
Gatekeeper Registration Failure	Indicates the endpoint could not register with the Polycom CMA system gatekeeper.
Internal System Errors	Indicates the endpoint is experiencing internal system errors.
ISDN Line Errors	Indicates the endpoint is experiencing ISDN line errors.
Endpoint Not Responding	Indicates the endpoint is not responding to system requests.
Camera Disconnected	Indicates the endpoint's camera is disconnected.
Microphone Disconnected	Indicates the endpoint's microphone is disconnected.
Low Battery in Remote	Indicates the battery in the endpoint's remote needs to be replaced.
Server Redirection	
UI Not Running	Indicates the endpoint's web address is not accessible.
Global Directory Server Registration Failure	Indicates the endpoint could not register with the Polycom Global Directory Server.

Alert Type	Description
Global Directory Server Connection Lost	Indicates the connection to the Polycom Global Directory Server has been lost.
Presence Server Registration Failure	Indicates the endpoint could not register with the presence server.
User Assistance Request	Indicates the endpoint user has a pending Help request.

3 Click **Update**.

Add a Remote Alert Profile

You can add a remote alert profile to identify which device alerts from which devices should be sent as part of a remote alert profile. Note that using a combination of setting alerts by device type and by specific types, provide additional granularity in managing device alerts.

To add a remote alert profile

1 Go to **Admin > Alert Settings > Remote Alert Profiles**.

2 On the **Remote Alert Profiles** page, click **Add**.

3 In the **Add Remote Alert Profile** dialog box, enter a **Name** and **Description** for the profile.

4 To activate the profile, select **Enable Profile**.

5 Configure one of the following:

- To have all Polycom CMA system alerts sent as part of this profile, select **Info**, **Minor**, *and* **Major**.
- To have a subset of Polycom CMA system alerts sent as part of this profile, select any combination of **Info**, **Minor**, or **Major**. These selections work in conjunction with the Polycom CMA system alert level settings you choose previously.
- To have no Polycom CMA system alerts sent as part of this profile, leave **Info**, **Minor**, *and* **Major** unselected**.**

6 To use the device type to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device Type** and configure one of the following. For endpoint systems, these selections work in conjunction with the endpoint alert level settings you choose previously.

a To have all device alerts for all device types sent as part of this profile:

In the **Device Type Alert Level Mapping** page, select **Info**, **Minor**, *and* **Major** for all of the device types.

b To have a subset of device alerts for all device types sent as part of this profile:

In the **Device Type Alert Level Mapping** page, select any combination of **Info**, **Minor**, or **Major** for each device type.

c To have all device alerts for a subset of device types sent as part of this profile:

In the **Device Type Alert Level Mapping** page, select **Info**, **Minor**, or **Major** for each device type to be included in the profile. Alerts for those device types that do not have an alert level selected will not be included.

7 To use the device name to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device**.

Notes

- If you set device alerts for specific devices, these settings override settings made on the **Alert by Device Type** page. The settings are not cummulative.
- You cannot set the system up to send device alerts for specific desktop video endpoints. Polycom CMA Desktop and Polycom PVX endpoints are not displayed in the **Available Device** list.

a As needed, use the **Filter** to customize the device list.

b In the **Available Devices** list, select the devices to add to the profile. Use **Ctrl** to select multiple devices.

c Click the down arrow to add the devices to the **Monitored Devices** list and configure one of the following:

d To have all device alerts for all selected devices sent as part of this profile:

For the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device.

e To have a subset of device alerts for all selected devices sent as part of this profile.

For the devices in the **Monitored Devices** list, select any combination of **Info**, **Minor**, or **Major** for each device.

f To have all device alerts for a subset of device types sent as part of this profile:

For the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device to be included in the profile. Alerts for those devices in the **Monitored Devices** list that do not have an alert level selected will not be included.

8 Click **OK**.

Associate a Remote Alert Profile With a User

To associate a remote alert profile with a user

1. Go to **User > Users**.
2. To search for a user:
   a. In the **Search** field of the **Users** page, search for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.

> **Note**
> Searches for a user on the Polycom CMA system **Users** page are case-insensitive, exact-match searches of the **Username**, **First Name**, and **Last Name** fields.

   b. To search both local and enterprise users, clear the **Local Users Only** checkbox and press **Enter**.

      The first 500 users in the database that match your search criteria are displayed in the **Users** list.

   c. If the list is too large to scan, further refine your search string.
3. Select the user of interest and click **Edit User**.
4. In the **Edit User** dialog box, click **Associated Alert Profile**.
5. Select the **Remote Alert Profile** to associate with the user.
6. Click **OK**.

Edit a Remote Alert Profile

To edit a Remote Alert Profile

1. Go to **Admin > Alert Settings > Remote Alert Profiles**.
2. On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.
3. As required, edit the **General Info**, **Alert by Device Type,** and **Alert by Device** sections of the **Edit Remote Alert Profile** dialog box.
4. Click **OK**.

Disable a Remote Alert Profile

To disable a Remote Alert Profile

1. Go to **Admin > Alert Settings > Remote Alert Profiles**.
2. On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.
3. Clear **Enable Profile**.
4. Click **Update**.

Delete a Remote Alert Profile

To delete a Remote Alert Profile

1. Go to **Admin > Alert Settings > Remote Alert Profiles**.
2. On the **Remote Alert Profiles** page, select the profile of interest and click **Delete Remote Alert Profile**.
3. Click **Yes** to confirm the deletion.

   The profile is deleted from the Polycom CMA system.

Disable Polycom CMA System Remote Alerts

To disable all (system and device) Polycom CMA System remote alerts

1. Go to **Admin > System Settings > Remote Alert Setup**.
2. On the **Remote Alert Setup** page, clear **Enable Remote Alerts**.
3. Click **Update**.

31

System Backup and Recovery Operations

This chapter describes the Polycom® Converged Management Application™ (CMA™) system management tasks. It includes these topics:

Overview of the Polycom CMA System Database

Polycom CMA system information is stored in these databases:

Database	Description
ReadiManager	The general Polycom CMA system database that includes all data for scheduling, devices, dial rules, device registration, and site topology
Logger	The Polycom CMA system database for call detail records and gatekeeper diagnostic logs
XMPP	The Polycom CMA system database for presence information

Database	Description
master model msdb	The Polycom CMA system Microsoft MSDE system databases

The Polycom CMA system automatically optimizes its internal database on an ongoing basis. It backs up its internal databases daily. The backup files are stored on the system's hard disk.

The Polycom CMA system maintains the last four internal backups. To keep backups for a longer time period, copy them regularly to a different location. For more information, see "Copy the Polycom CMA System Database Backup Files" on page 332.

Manually Backup a Polycom CMA System

You can also perform manual backups and restore existing backups through the Polycom CMA system serial console or Microsoft Enterprise Manager. As a best practice, only do backups during a maintenance window when there are no active conferences.

Note

If you set up an external database, follow your own corporate policies (or Microsoft best practices) to back it up and maintain it. The Polycom CMA system does not backup external databases.

To perform a manual backup:

1. Connect to the Polycom CMA System Serial Console.
2. Backup the Polycom CMA System Databases.
3. Copy the Polycom CMA System Database Backup Files.

You can back up databases as follow.

From ...	To ...
Internal	Internal
Internal	External
External	External

Connect to the Polycom CMA System Serial Console

To connect to the Polycom CMA system serial console

1. Connect a computer to the Polycom CMA system server through the RS-232 serial port.
2. Power on the computer.
3. Access the serial console and start a **Hyperterm** session.
4. In the **Connection Description** dialog box, type Polycom CMA in the **Name** field and click **OK**.
5. In the **Connect To** dialog box, select **COM1** in the **Connect using** drop-down list and click **OK**.
6. In the **Properties** dialog box, enter these values for port settings.
   - **Bits per second:** 19200
   - **Data bits:** 8
   - **Parity:** None
   - **Stop bits:** 1
   - **Flow control:** None

   The **Polycom CMA Administrative Console** appears.

Backup the Polycom CMA System Databases

As a best practice, only do backups during a maintenance window when there are no active conferences.

To back up a database from the Polycom CMA server serial port

1. Connect to the Polycom CMA system serial console, as described in "Connect to the Polycom CMA System Serial Console" on page 331.
2. In the starting menu, select **`(4) Database Operations`**.
3. In the **Database Operations** menu, select **(1) Backup Local Databases**.

   If you have a previous backup that you created earlier, a warning appears stating: "`The following backup database files will be deleted. To keep these files, enter 'N' to exit and then use the Copy Database operation to copy them to an external location. Do You Wish to Continue?`"

- To save a previous backup, select **N** and then select **(4) Copy Database files TO ...** to copy these files to an external location. See "Copy the Polycom CMA System Database Backup Files" on page 332.
- To delete the previous backup database files, select **Y**.

4 When prompted, enter the administrator user name and password.

The system backs up the database. When the backup is complete, a success message for the completed backup displays on the console.

Copy the Polycom CMA System Database Backup Files

In addition to backing up and restoring database files, you can copy the database backup files to and from the Polycom CMA system to an external location.

You have two options for copying the Polycom CMA system backup files: the Polycom CMA system web interface and the Polycom CMA system serial console. Copying the database backup files using the web interface saves them to a local system. Copy them using the serial port puts them on a USB drive. You can also use the Polycom CMA system serial port to copy the database backup file onto the Polycom CMA system.

To copy the Polycom CMA system database backup files using the web interface

1 Go to **Admin > Database Backup Files**.

The **Database Backup Files** list appears showing all of the backup files stored on the Polycom CMA system. Files with a timestamp included in the name are system-generated backup files. Files without a timestamp are user forced backups.

2 In the **Database Backup Files** list, select the backup files of interest and click **Save**.

3 In the **Save As** dialog box, browse to a location and click **Save**.

To copy the database backup files from the Polycom CMA system onto a USB flash drive

1 Connect to the Polycom CMA system serial console, as described in "Connect to the Polycom CMA System Serial Console" on page 331.

2 In the **Root** menu, select **4. Database Operations**.

3 In the **Database Operations** menu, select **4. Copy Database files TO ...**.

4 Select the source and destination locations to copy database files.

Note

Make sure you create a folder for the database backup files before you copy the files or the operation will fail.

5 Enter the full path of the folder to which the database files will be copied. For example, if the folder is on the root, type backslash (\).

The system copies the files. When the backup is complete, the **Database Operations** menu reappears.

6 Exit the serial console.

To copy the database backup files to the Polycom CMA system from a USB flash drive

1 Connect to the Polycom CMA system serial console, as described in "Connect to the Polycom CMA System Serial Console" on page 331.

2 In the **Root** menu, select **4. Database Operations**.

3 In the **Database Operations** menu, select **3. Copy Database files FROM...**.

4 Select the source location on the USB flash drive from which you want to copy database files.

5 Enter the full path and file name of the database backup files (`.bak`) or just the file names if they are on the root.

The system copies the files. When the backup is complete, the **Database Operations** menu reappears.

6 Exit the serial console.

Overview of Database Restoration

To restore an internal Polycom CMA system database, follow the procedures in this section. To restore an external Microsoft SQL Server databases, use Microsoft SQL Server Management Studio. Refer to your Microsoft SQL Server Management Studio documentation for more information.

When you restore internal or external databases:

- Do not allow users to connect to the server during the restoration process
- Restore all of the system databases at the same time
- Restore all of the system databases from backups that were taken at the same time
- Restart the Polycom CMA system server when the restoration process is finished

Restore the Polycom CMA System Internal Databases

To restore the Polycom CMA system internal databases

1. Back up the databases as described in "Backup the Polycom CMA System Databases" on page 331.
2. When the **Database Operations** reappears on the Polycom CMA system serial console, select **`2. Restore Local Databases`**.
3. When prompted, enter the database name.
4. Enter the administrator username and password.

   A list of database backup files appear, with corresponding backup dates.
5. Select the number of the database backup file to restore.

   The system restores the database. When the restoration is complete, a success message for the completed backup displays on the console and the **Database Operations** menu reappears.
6. Repeat step 5 to restore the next database backup file.
7. After you have restored all of the databases, exit the serial console and restart the Polycom CMA system server.

Restore the Polycom CMA System External Database

You can restore an external Microsoft SQL Server database using Microsoft SQL Server Management Studio or Microsoft SQL Query Analyzer.

> **Note**
> The database name is part of each backup file name. Make sure you restore the correct backup file for each database.

To restore external databases

1. Restore all of the Polycom CMA system database backup files as described in "Restore the Polycom CMA System Internal Databases" on page 334.
2. Run the following command using Microsoft SQL Server Management Studio or Microsoft SQL Query Analyzer.

   ```
   EXEC ReadiManager.dbo.pr_FixOrphanUsers
   ```
3. Restart the Polycom CMA system server.

Recovery Operations - Reset First Time Setup

To recovery after a disaster, you must **Reset First Time Setup**. This:

- Re-enables the **First Time Setup** pages
- Allows you to reconfigure the Polycom CMA system network, database, and LDAP settings

Note

Reset First Time Setup preserves all user data and does not change any configuration settings, such as licenses, system, network, database, or LDAP.

To reset First Time Setup

Note

Before you reset the **First Time Setup** pages, make sure you know a valid Polycom CMA system administrator username and password. You'll need it to log into the Polycom CMA system and the factory-set username and password may have changed.

1. Connect to the Polycom CMA system serial console, as described in "Connect to the Polycom CMA System Serial Console" on page 331.
2. On the **Root** menu, select **6. Disaster Recovery**.
3. Select **1. Reset First Time Setup**.

   The system resets itself to its first time setup state. When the reset is complete, a success message displays on the console.
4. Exit the serial console.
5. Review the **First Time Setup** pages and make required changes to any settings.

   The system is restored and is ready for use.

Restart or Orderly Shut Down a Polycom CMA System

You have several options when performing an orderly shut down of a Polycom CMA system in non-emergency situations. You can stop future scheduled conferences from starting automatically on the system, wait for active conferences to end, and then either **Shutdown** the system or **Restart** the system. They include:

- Press once, but do not hold, the power switch on the rear panel of the Polycom CMA system server. This is equivalent to selecting the **Shutdown** option (described next).
- Use the **Shutdown** option when you must disconnect the Polycom CMA system server for some reason, e.g., to move it. All Polycom CMA system functionality is stopped during a **Shutdown**.
- Use the **Restart** option when you must cycle the Polycom CMA system for some reason, e.g., if the system locks up.
- During a restart, the system will drop all IP conferences. In general, ISDN conferences will not drop. Also, devices registered to the gatekeeper will drop. IP devices not registered with the gatekeeper can continue in conference.

To restart or orderly shut down a Polycom CMA system

1. (Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:
   a. Go to **Admin > Conference Settings**.
   b. Check the **Conference Auto-Launch Disabled** checkbox and click **Update**.
   c. Go to **Admin > Dashboard**.
   d. Monitor the **Today's Conferences** section to determine when all active conferences are completed.
2. Click **Restart**  or **Shutdown**  , as required.

   In a redundant Polycom CMA system configuration, the system displays a warning indicating that it is initiating a failover.

   If you select **Restart**, it may take the Polycom CMA system up to 10 minutes to shutdown and then restart all server processes.

Emergency Shut Down of a Polycom CMA System

You have two options to perform an emergency shut down of a Polycom CMA system. Use these options only when you must immediately cut power to the server.

- Press and hold the power switch on the rear panel of the Polycom CMA system server.
- Pull the system power cord.

After an emergency shutdown (i.e. when you press and hold the power switch, or you pull the system cord, or you lose power to the system), a system battery may continue to cache information until the battery runs out. In this case, the system enters an error state. To recover, you must connect a keyboard and monitor to the Polycom CMA system and boot the system to clear the error message. Then the system can begin recovery.

Disaster Recovery - Restore to Factory Default Image

In a disaster recovery situation, your Polycom Global Services (PGS) support representative may instruct you to restore your Polycom CMA system to its factory default image.

To perform this disaster recovery procedure, you will need the **Restore to Factory Default DVD** that shipped with the Polycom CMA system server. This DVD has the base image of the Polycom CMA system server software.

WARNING

- This is a last resort, so never do this without being instructed to do so by PGS support.
- This procedure will wipe out your system database and all other system data.
- The **Restore to Factory Default DVD** is specifc to the Polycom CMA system server type: either 4000 or 5000.

32

System Troubleshooting

This chapter has Polycom® Converged Management Application™ (CMA™) system troubleshooting information. It includes the following topics:

Note
Some recommended solutions require access to pages in the Administrator View. The default Scheduler or Operator permissions do not provide access to this view. You must log in as and administrator to access this view.

Registration Problems and Solutions

Problem	Description	Solutions
Unable to place calls to an MCU conference room from a registered Polycom HDX system	The Polycom CMA system rejects the ARQ stating that the "endpoint is not registered" to the gatekeeper even though the system indicates it is registered.	• The MCU is not registered to the gatekeeper
When the gatekeeper registration is set to auto-discovery, endpoints do not register.	When auto-discovery is used, a GRQ message is broadcast and sent over multicast. However, the Polycom CMA system must be able to receive one of these messages, and does not respond to this message if it is not the default gatekeeper.	• Verify that the Default Gatekeeper check box is selected in the **Admin > Gatekeeper Settings > Primary Gatekeeper** page. • Verify that a UDP broadcast from the endpoint's network can reach the Polycom CMA system, or that multicast is enabled on all routers between the endpoint and the Polycom CMA system.

Problem	Description	Solutions
An endpoint cannot register with the Polycom CMA system.	The endpoint is configured to use the Polycom CMA system as its gatekeeper, but is being rejected during registration. In the gatekeeper diagnostic log, an error has occurred during the RRQ/RCF process that caused the registration to fail.	• Review the gatekeeper diagnostic logs for the RRQ attempt by the endpoint and determine the RRJ reason. • Verify that the endpoint alias is not a duplicate of other endpoint aliases. • Verify that the endpoint does not have NAT enabled. • Verify that enough licenses remain.
An endpoint cannot register with the Polycom CMA system.	An endpoint cannot register with CMA, but the gatekeeper diagnostics do not indicate a problem. The gatekeeper sent the RCF message, but the endpoint did not receive it.	• Verify that the IP address that the gatekeeper sent to the endpoint is correct.
The MCU cannot register with the Polycom CMA system.	Some MCU vendors register with a GRQ message instead of an RRQ message. Some MCU vendors do not retry registration after a first attempt has failed.	• Verify that the Default Gatekeeper check box is selected in the **Admin > Gatekeeper Settings > Primary Gatekeeper** page. • Reset the MCU or MGC card to force registration to occur.
An endpoint shows that it is not registered to the gatekeeper in the **Gatekeeper Registration** field in the **Device Status**.	The Polycom CMA system receives the RRQ message, but not the LWRRQ message from the endpoint. The endpoint did not send a LWRRQ message within the offline timeout period specified in the **Admin > Gatekeeper Settings > Primary Gatekeeper** page.	• Reboot the endpoint.
The RadVision OnLAN MCU continually changes state: from online to offline and offline to online.	The Radvision OnLAN MCU ignores the RCF Time to Live (TTL) field, which is filled in with the value that the administrator specified in the offline timeout field in the **Admin > Gatekeeper Settings > Primary Gatekeeper** page.	• Reconfigure the Radvision OnLAN MCU to send the registration requests in the same time period specified in CMA. • Add the MCU manually. • Reboot the MCU to force registration to occur.

Problem	Description	Solutions
Some endpoints are not assigned ISDN numbers.	A registered H.323-only system was not assigned an ISDN number. The system could belong to a network that does not have ISDN number ranges assigned to it. No ISDN numbers are available to assign.	• Verify that the endpoint belongs to the site that has assigned ISDN number ranges. To do so, go to **Admin > Dial Plan and Sites > Sites** and make sure the site has the correct ISDN range specified in the **ISDN Number Assignment** pane. • Verify that ISDN numbers are available to assign. • Verify that the RCF message “Can’t find ISDN free pool” from the gatekeeper returns to the endpoint.
Endpoints that were previously registered and auto-assigned ISDN numbers are being rejected when attempting to register.	Inconsistent configuration in ISDN number assignment has occurred.	• Verify that the previous ISDN range was changed.
When the Polycom CMA system is restarted, some registrants that were previously online are now offline.	Some endpoints do not reregister when the Polycom CMA system goes down. Some MCUs do not reregister automatically after two retries.	• Reboot the MCU.

Point-to-Point Calling Problems and Solutions

Problem	Description	Solutions
ViewStation and ViaVideo have an incorrect RAS IP address.	These endpoints are configured with a NAT address and may not receive the RCF message from the gatekeeper.	The endpoints need to be reconfigured to disable NAT.
A call with an alias as the dial string from a registered endpoint cannot be placed to another registered endpoint. The two endpoints are in different sites.	• The site link between the sites in which the endpoints reside is not correctly defined or is missing. • No bandwidth is available to the site link. • The calling bit rate is higher than the bit rate defined in the site link. • ISDN alternate routing is not available. • Dialing rules may not be enabled or may be set to block instead of route.	• Go to **Admin > Dial Plan and Sites > Site Links** and make sure that a site link exists between the two networks. • Make sure that the IP addresses of both endpoints are included in their respective sites. • If site topology is defined for both endpoints, verify that there is enough bandwidth in the site links between the two sites. • Verify that the dialing bit rate is lower or equal to that of the maximum bit rate defined for the site links. • If the endpoint is ISDN capable, verify that the ISDN parameter is correct.
Dialing by IP address fails.	A registered endpoint cannot call an unregistered endpoint by IP address within the same site. A dialing rule is not enabled or is set to block instead of route.	• Check the **Reports > Gatekeeper Message Log** for error messages. • Verify that the registered endpoint is registered. • Verify that the **Deny calls to/from unregistered endpoints** check box is cleared. Go to **Admin > Gatekeeper Settings > Primary Gatekeeper** to change this setting. • Verify that the IP address dialing rule is enabled and set to route.

MCU and Gateway Dialing Problems and Solutions

Problem	Description	Solutions
Call fails when using an MCU service. Dialing an MCU service results in a network error.	The call using the MCU service is rejected because of one of the following: • The MCU is not registered. • The MCU is offline. • The MCU prefix is not registered as an E.164 alias. • The MCU resource issue was sent through resource allocation indication or resource allocation. • The dialing rule is not enabled. • The priority of the dialing rule may be too high. • Services are not enabled.	• Check the **Reports > Gatekeeper Message Log** for error messages indicating why the call failed. • Verify that the MCU is registered. • Verify that the MCU is online. If the device is offline, reboot it. • Verify that the MCU service is available. Go to the **Admin > Dial Plan and Sites > Services** page. Verify that the MCU service prefix is enabled and listed.
Simplified dialing does not work. When you dial 9, you receive a network error.	The call using the simplified dialing service is rejected because of one of the following: • The simplified dialing prefix service in the system configuration is disabled. • No gateway services are available. • There is insufficient BRI/PRI bandwidth. • The call uses a higher bit rate than the device policy group allows.	• Check the **Reports > Gatekeeper Message Log** for error messages. • Verify that the gateway and simplified dialing service prefix is enabled. Go to **Admin > Dial Plan and Sites > Services**. • Verify that the gateway is registered.

Conference On Demand Problems and Solutions

Problem	Description	Solutions
Dialing a Conference On Demand fails. Inviting other endpoints into a conference using the CON service fails.	The endpoint dials a CON service, and the call is rejected because of one of the following: • The MCU is not registered or is offline. • The Polycom CMA system cannot log into the MGC. • The MGC has no resource available for the call. • The MGC's IP address is not entered in the Polycom CMA system.	• Check the diagnostics log for an ARJ reason from this endpoint. • Verify that the MCU is registered with the Polycom CMA system and is online. • Verify that the MCU registered with the Polycom CMA system has the MCU's IP address filled out in the **Devices** list. • Verify that the MCU login ID and password for the CON service are correct. • Verify that the H.323 network service that the MCU is using is set as the default service. • Verify that the MCU has enough available resources to start this conference. • Verify that the CON service is enabled. Go to **Admin > Dial Plan and Sites > Services**.

Gatekeeper Cause Codes

Cause Code	Description
150	The gatekeeper is out of resources
151	The gatekeeper has insufficient resources
152	The gatekeeper registration version is invalid
153	The call signal address is invalid
154	The registering device's address is invalid
155	The registering device's terminal type is invalid
156	The registering device's permissions are invalid
157	The conference ID is invalid
158	The The registering device's ID is invalid
159	The caller's device is not registered

Cause Code	Description
160	The called party's device is not registered
161	The registering device's permissions have expired
162	The registering device has a duplicate alias
163	The call transport is not supported
164	The called deivce has a call in progress
165	The call has been routed to the gatekeeper
166	Cannot request a drop for others
167	The registering device is not registered with the gatekeeper
168	Unknown reason
169	Permission failure
170	Discovery permissions have expired
171	The device is not registered
172	No bandwidth available
173	Location not found
174	Security access denied
175	Quality of service not supported
176	Resources are exhausted
177	Invalid alias
178	Cannot unregister others
179	Quality of service control is not supported
180	Incomplete address
181	Registration permissions have expired
182	Call routed to SCN
183	Inconsistent alias
203	Call rejected at destination
208	Incorrect address
221	The far end is busy
222	The far end is not responding

A

System Security and Port Usage

This section provides an overview of the port usage and security required by the Polycom® Converged Management Application™ (CMA™) system system and includes a comprehensive list of services and clients on the system that are required for normal operation.

Port Usage

The Polycom CMA system in this release is designed to sit behind your corporate firewall. The following sections describe inbound and outbound ports on the Polycom CMA system.

Open Inbound Ports on the Polycom CMA System

The following table lists the open ports on the Polycom CMA system and provides a description of their use.

Port	Description
TCP 80	HTTP web server, through which the web application displays and where Polycom endpoints post status messages
UDP 123	Network Time Protocol (NTP) listener
TCP 135	Microsoft RPC listener
TCP/UDP 137	NetBIOS name service listener
TCP/UDP 139	NetBIOS SMB listener
TCP/UDP 161	SNMP listener
TCP 389	Directory services (LDAP)
TCP 443	HTTPS web server listener
TCP 700	Service monitor for redundant Polycom CMA servers

Port	Description
TCP 1042	.NET listener used for the Microsoft SQL Server
TCP 1063	.NET listener
TCP/UDP 1167	.NET listener
TCP/UDP 1433	Internal MSDE server listener on this port, which enables views into the database from outside the Polycom CMA system
TCP/UDP 1720	The gatekeeper listener for RAS messages
TCP 2773	Codec manager for remote control of iPower endpoints
TCP 3601	Global Address Book listener with which endpoints register
TCP 5222	Presence service (XMPP)
TCP 8085-8088	.NET listener for remote access

Outbound Ports Used by the Polycom CMA System

The following table lists all outbound ports that the Polycom CMA system uses to communicate with other systems, including endpoints, bridges, database servers, and other network equipment.

Port	Description
TCP 20	Used to FTP data to endpoints
TCP 21	
TCP/UDP 24	Used to access the telnet interfaces on endpoints
TCP/UDP 25	Used to send email messages to SMTP servers
TCP/UDP 53	Used to access domain name servers (DNS)
TCP 80	Used to access the web application on endpoints and MGCs, version 7.x and higher
TCP 135 TCP 137 TCP 139	Active Directory Single Signon (NetBios/NTLM)
TCP/UDP 389	Used to access LDAP services
TCP 443	Secure access to endpoint devices (SSL) including CMA Desktop
TCP 445	Active Directory Single Signon
TCP 1205	Used to access MGCs for management and monitoring

Port	Description
TCP/UDP 1719	Used by the gatekeeper for H.323 datagrams
TCP/UDP 1720	Used by the gatekeeper for H.323 RAS messages
TCP/UDP 3268	Used to access the Active Directory Global Catalog
TCP 5001	Used to access MGCs for management and monitoring
TCP 5222	Presence service (XMPP)

B

System Field Input Requirements

The text input fields in each Polycom® Converged Management Application™ (CMA™) system page accept basic ASCII, extended-ASCII (eASCII), or Unicode input as indicated in the following table.

Field	Data Format	Page
Filter Value: Owner	Unicode	Conference view > Secondary Filter
Filter Value: Conference Name	Unicode	Conference view > Secondary Filter
Conference Name	Unicode	Add/Edit Conference
Last Name	Unicode	Add/Edit Conference > Add Participants
First Name	Unicode	Add/Edit Conference > Add Participants
Name	Unicode	Add/Edit Conference > Add Guest
Email	ASCII(1)	Add/Edit Conference > Add Guest
Number	N/A	Add/Edit Conference > Add Guest > Dial-Out + IP | ISDN Note Entry of text-based IP alias values is prohibited.
To	ASCII	Add/Edit Conference > Email Notification
CC	ASCII	Add/Edit Conference > Email Notification
BCC	ASCII	Add/Edit Conference > Email Notification
Additional Notes	Unicode	Add/Edit Conference > Email Notification
Filter Value: Name	ASCII	Endpoint > Monitor View Network Device > Monitor View
Filter Value: Alias	ASCII	Endpoint > Monitor View Network Device > Monitor View
Filter Value: Site	Unicode	Endpoint > Monitor View Network Device > Monitor View
Admin ID	ASCII	Add/Edit Device > Find Device on Network

Field	Data Format	Page
Password	ASCII(15)	Add/Edit Device > Find Device on Network
System Name	ASCII(2)	Add/Edit Device > Identification
Description	eASCII	Add/Edit Device > Identification
Serial Number	ASCII	Add/Edit Device > Identification
Software Version	ASCII	Add/Edit Device > Identification
HTTP URL	ASCII	Add/Edit Device > Identification
HTTP Port	Numeric	Add/Edit Device > Identification
DNS Name	ASCII	Add/Edit Device > Addresses
Alias Value (E164)	0 through 9, *, and #	Add/Edit Device > Addresses
Alias Value (H323 ID)	ASCII	Add/Edit Device > Addresses
Alias Value (URL)	ASCII	Add/Edit Device > Addresses
Alias Value (Transport Address)	ASCII	Add/Edit Device > Addresses
Alias Value (Party Number)	Numeric	Add/Edit Device > Addresses
Alias Value (Unknown)	ASCII	Add/Edit Device > Addresses
Service Name	ASCII	Add/Edit Device > MCU Services > Add > Gateway | H320 | H323
Dialing Prefix	Numeric	Add/Edit Device > MCU Services > Add > Gateway | H323
Channels	Numeric	Add/Edit Device > MCU Services > Add > H320
Number Range	0 through 9 and '-' (dash)	Add/Edit Device > MCU Services > Add > H320
Service IP Address	0 through 9 and '.' (period)	Add/Edit Device > MCU Services > Add > H323
Alias	E164	Add/Edit Device > MCU Services > Add > H323
Message Text	ASCII	Endpoint > Monitor View > Send Message | Clear Help
Filter Value: Name	ASCII	Endpoint > Softupdate View > Filter
Filter Value: Alias	ASCII	Endpoint > Softupdate View > Filter
Filter Value: Site	Unicode(9)	Endpoint > Softupdate View > Filter
Name	Unicode(5)	Add/Edit Conference Template
Description	ASCII	Add/Edit Conference Template
RMX Profile Name		Add/Edit Conference Template

Field	Data Format	Page
Talk Hold Time	Numeric x.x to y.y	Add/Edit Conference Template
From Address	ASCII	Conference Settings
SMTP Server		Conference Settings
Filter Value: First Name	Unicode	Users > Attribute Filter
Filter Value: Last Name	Unicode	Users > Attribute Filter
Filter Value: User ID	Unicode	Users > Attribute Filter
First Name	Unicode(6)	Add/Edit User
Last Name	Unicode	Add/Edit User
User ID	Unicode	Add/Edit User; AND Login Page
Password/Confirm Password	Unicode(7)	Add/Edit User; AND Login Page
Email Address	Unicode(8)	Add/Edit User
Search Value	Unicode	Add Room > Search LDAP by First Name | Last Name | User ID
Description	ASCII	Add/Edit Room > General Info
Email	Unicode(8)	Add/Edit Room > General Info (display of LDAP email address or entry of a Local email address)
Filter Value: Device Name	ASCII	Global Address Book > Attribute Filter
Name	ASCII(10)	Add GAB User
E-164 Alias	0 through 9, *, and #	Add GAB User > IP Video
IP Address	IP Address format	Add GAB User > IP Video
City Code	Numeric	Add GAB User > ISDN Video
Number A	Numeric	Add GAB User > ISDN Video
Number B	Numeric	Add GAB User > ISDN Video
Extension	Numeric	Add GAB User > ISDN Video
Old Password	ASCII(11)	Set GAB Password
New Password / Confirm	ASCII	Set GAB Password
Filter Value: Name	ASCII(2)	Provision Device Profiles
Filter Value: Created By	Unicode(12)	Provision Device Profiles

Field	Data Format	Page
Admin Password	ASCII	Add/Edit Provision Profile > General Settings > Security
Meeting Password	ASCII	Add/Edit Provision Profile > General Settings > Security
Country Code	E164	Add/Edit Provision Profile >Video Network > IP Network > Gateway Number
Area Code	E164	Add/Edit Provision Profile >Video Network > IP Network > Gateway Number
Gateway Number	E164	Add/Edit Provision Profile >Video Network > IP Network > Gateway Number
Outside Line Dialing Prefix	E164	Add/Edit Provision Profile >Video Network > IP Network > ISDN BRI Protocol
Camera 1 Name	ASCII	Add/Edit Provision Profile > Cameras
Camera 2 Name	ASCII	Add/Edit Provision Profile > Cameras
Camera 3 Name	ASCII	Add/Edit Provision Profile > Cameras
Host Name	ASCII	Add/Edit Provision Profile > LAN Properties > LAN Properties 1
Password	ASCII	Add/Edit Provision Profile > Global Services > Directory Servers
Number of digits in Extension	Numeric	Add/Edit Provision Profile > Global Services > Dialing Rules 1
International Dialing Prefix	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 1
Public Network Dialing Prefix	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 1
Public Network (same area code) Prefix	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 1
Private Network Dialing Prefix	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 1
If Area Code Equals	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 2
Dial Prefix	E164	Add/Edit Provision Profile > Global Services > Dialing Rules 2
Contact Person	ASCII	Add/Edit Provision Profile > Global Services > My Information
Contact Number	E164	Add/Edit Provision Profile > Global Services > My Information
Contact Email	ASCII	Add/Edit Provision Profile > Global Services > My Information

Field	Data Format	Page
Contact Fax	E164	Add/Edit Provision Profile > Global Services > My Information
Tech Support	ASCII	Add/Edit Provision Profile > Global Services > My Information
City	ASCII	Add/Edit Provision Profile > Global Services > My Information
State/Province	ASCII	Add/Edit Provision Profile > Global Services > My Information
Country	ASCII	Add/Edit Provision Profile > Global Services > My Information
Software Update Key File	ASCII	Software Update Profile > Upload Software Update
Description	ASCII	Software Update Profile > Upload Software Update
Filter Value: Name	ASCII(2)	Software Update Profiles > Get Serial Numbers
Filter Value: Site	Unicode	Software Update Profiles > Get Serial Numbers
Get Serial Numbers text box	ASCII	Software Update Profiles > Get Serial Numbers
Filter Value: Name	ASCII	User Roles
Filter Value: Description	ASCII	User Roles
Name	ASCII	User Roles > Add/Edit Role
Description	ASCII	User Roles > Add/Edit Role
Filter Value: Group Name	Unicode(13)	User Roles for LDAP Groups
Filter String	ASCII	Reports > Gatekeeper Message Log
Filter Value: IP Address	IP Address	Reports > IP Call Detail Records
Filter Value: System Name	ASCII(2)	Reports > ISDN Call Detail Records
System Name	ASCII(14)	Server Settings > Network
IP Address	IP Address	Server Settings > Network
Subnet Mask	Subnet Mask	Server Settings > Network
Default Gateway	IP Address	Server Settings > Network
DNS Server	IP Address	Server Settings > Network
IP Address or DNS Name	ASCII	Server Settings > System Time > External NTP Server Time Synchronization
DB Server IP Address	IP Address	Server Settings > Database
DB Server Port	Numeric	Server Settings > Database
DB Instance Name	ASCII	Server Settings > Database

Field	Data Format	Page
LDAP Server IP Address or DNS Name	ASCII	Server Settings > LDAP
LDAP User ID	Unicode	Server Settings > LDAP
LDAP User Password	Unicode(7)	Server Settings > LDAP
Activation Key	ASCII	Server Settings > Licenses
Virtual IP	IP Address	Server Settings > Redundant Configuration
Server IP	IP Address	Server Settings > Redundant Configuration
Gatekeeper Identifier	ASCII	Gatekeeper Settings > Primary Gatekeeper
Gatekeeper Description	ASCII	Gatekeeper Settings > Primary Gatekeeper
Alternate Gatekeeper ID	ASCII	Gatekeeper Settings > Alternate Gatekeeper
IP Address	IP Address	Gatekeeper Settings > Alternate Gatekeeper
Port	Numeric	Gatekeeper Settings > Alternate Gatekeeper
Priority	Numeric	Gatekeeper Settings > Alternate Gatekeeper
Country Name (2 letter code)	ASCII	Security Settings > Generate Certificate Request
State or Province Name	ASCII	Security Settings > Generate Certificate Request
Locality Name	ASCII	Security Settings > Generate Certificate Request
Organization Name	ASCII	Security Settings > Generate Certificate Request
Organizational Unit Name	ASCII	Security Settings > Generate Certificate Request
Common Name	ASCII(14)	Security Settings > Generate Certificate Request
Email Address	ASCII	Security Settings > Generate Certificate Request
Password / Verify Password	ASCII(15)	Security Settings > Endpoint Management Settings
Site Name	Unicode(9)	Dial Plan > Sites > Add/Edit Site
Description	ASCII	Dial Plan > Sites > Add/Edit Site
PBX Access Code	E164	Dial Plan > Sites > Add/Edit Site
Name	ASCII	Dial Plan > Site-Links > Add/Edit Site-Link
Description	ASCII	Dial Plan > Site-Links > Add/Edit Site-Link
Name	ASCII	Dial Plan > Gatekeeper Regions > Add/Edit Region
Description	ASCII	Dial Plan > Gatekeeper Regions > Add/Edit Region
Gatekeeper IP Address	IP Address	Dial Plan > Gatekeeper Regions > Add/Edit Region
Gatekeeper Identifier	ASCII	Dial Plan > Gatekeeper Regions > Add/Edit Region
Description	ASCII	Dial Plan > Services > Add/Edit Service > General Info

Field	Data Format	Page
Service Prefix	ASCII	Dial Plan > Services > Add/Edit Service > General Info
Insert between Prefix & First number	E164	Dial Plan > Services > Add/Edit Service > Simplified Dialing
Insert between Phone number	E164	Dial Plan > Services > Add/Edit Service > Simplified Dialing
Append after full Dial string	E164	Dial Plan > Services > Add/Edit Service > Simplified Dialing
Login ID	ASCII	Dial Plan > Services > Add/Edit Service > Conference On Demand
Password	ASCII	Dial Plan > Services > Add/Edit Service > Conference On Demand
H.323 Network Service	ASCII	Dial Plan > Services > Add/Edit Service > Conference On Demand
RMX Profile Name	Unicode	Dial Plan > Services > Add/Edit Service > Conference On Demand
Name	ASCII	Dial Plan > Dial Rules > Add/Edit Rule > General Information
Description	ASCII	Dial Plan > Dial Rules > Add/Edit Rule > General Information
IP Address Pattern Data	ASCII	Dial Plan > Dial Rules > Add/Edit Rule > Routing Action
Name	ASCII	Dial Plan > LCR Tables > Add/Edit LCR
Description	ASCII	Dial Plan > LCR Tables > Add/Edit LCR
Alert Note	ASCII	System Alerts > Edit

Index

D

E

F

G

H

I

K

L

R

S

T

U

V

W

Y