Contents

1 Polycom® CMA™ System Overview
   Features and Capabilities ................................................. 1
   Minimum System Requirements ...................................... 2
   Other Requirements ..................................................... 2
   Log Into the Polycom CMA System .................................. 2
   Log Out of the Polycom CMA System ............................... 3
   Working in the Polycom CMA System ............................... 4
      Polycom CMA Site Map ............................................... 4
      Polycom CMA System Views, Roles, and Permissions .......... 5
      Field Input Requirements ........................................... 6
      Filter and Search a List ............................................ 6
   Managing Bandwidth ................................................... 7

2 Polycom® CMA™ System Configuration
   Add DNS SRV Record for Polycom CMA Services ............... 9
   Configure Redundancy .................................................. 10
      Configure the External Database for Redundancy .......... 10
      Set the Virtual IP Address for the Redundant System .... 11
   License the Polycom CMA System .................................. 12
   Configure the Connection to the External Database .......... 13
   Configure the Connection to an External Enterprise Directory . 13
   Set Up Video Call Routing ............................................ 13
   Set Up Automatic Device Provisioning ............................ 14
   Set Up Automatic Softupdate ......................................... 15
   Set Up Conference Templates ......................................... 15
   Set Up Directory Services .............................................. 15
   Distribute Polycom Applications ................................. 16

3 Conference Scheduling Overview
   Schedule Conference View ............................................. 21
   Monitor Conf View ........................................................ 22
   Conference Commands .................................................. 23
4 Conference Management Operations

Add a Conference .................................................. 25
Delete a Conference .............................................. 29
Edit a Conference .................................................. 30
Edit a Participant’s Settings ................................. 31
Edit a Room’s Settings ......................................... 32
Manage an Active Conference ......................... 33
Manage a Participant Device During a Conference ...... 35

5 Advanced Conference Settings

Advanced Conference Settings ............................... 37
Edit Advanced Conference Settings ...................... 40

6 Conference and Participant Fields

Conference List ..................................................... 41
Conference Details .............................................. 42
Conference Features ............................................ 44
Bridge (MCU) Features ........................................ 46
Participants ......................................................... 47
Participant Details .............................................. 47
Participant Settings .............................................. 48
Manage Conference - Participants List .................. 50

7 Device Management Overview

Device Menu, Views, and Lists ............................... 51
Admin/Monitor View ............................................. 52
Device List in the Admin/Monitor View ................. 52
Commands in the Admin/Monitor View ................. 53
Automatic Provisioning View .............................. 54
Device List in the Automatic Provisioning View ...... 54
Commands in the Automatic Provisioning View ...... 55
Scheduled Provisioning View ............................... 56
Device List in the Scheduled Provisioning View ...... 56
Commands in the Scheduled Provisioning View ...... 57
Automatic Softupdate View ................................. 58
Device List in the Automatic Softupdate View ........ 58
Commands in the Automatic Softupdate View ........ 59
Scheduled Softupdate View ................................. 59
Device List in the Scheduled Softupdate View ...... 59
Scheduled Softupdate View Commands ................ 60
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Types</td>
<td>61</td>
</tr>
<tr>
<td>Device Configuration/Provisioning</td>
<td>62</td>
</tr>
<tr>
<td>Automatic Device Provisioning</td>
<td>63</td>
</tr>
<tr>
<td>How Automatic Device Provisioning Works</td>
<td>63</td>
</tr>
<tr>
<td>Automatic Provisioning Profiles</td>
<td>63</td>
</tr>
<tr>
<td>Profile Order and Priority</td>
<td>65</td>
</tr>
<tr>
<td>Scheduled Device Provisioning</td>
<td>65</td>
</tr>
<tr>
<td>How Scheduled Device Provisioning Works</td>
<td>66</td>
</tr>
<tr>
<td>Scheduled Provisioning Profiles</td>
<td>66</td>
</tr>
<tr>
<td>Device Softupdates</td>
<td>67</td>
</tr>
<tr>
<td>Automatic Device Softupdates</td>
<td>67</td>
</tr>
<tr>
<td>How Automatic Device Softupdate Works</td>
<td>68</td>
</tr>
<tr>
<td>Automatic Softupdate Profiles</td>
<td>68</td>
</tr>
<tr>
<td>Automatic Softupdate Versions</td>
<td>68</td>
</tr>
<tr>
<td>Scheduled Device Softupdates</td>
<td>69</td>
</tr>
<tr>
<td>Device Passwords</td>
<td>70</td>
</tr>
</tbody>
</table>

#### 8 Device Management Operations

- View Device Details                                                 | 71   |
- Add an Endpoint or Find an Endpoint on the Network                   | 72   |
- Add an MCU Manually                                                  | 76   |
- Edit a Device                                                       | 79   |
- Delete a Device                                                     | 80   |
- View a Device’s Video Feed                                          | 80   |
- Clear a Device Help Request                                         | 81   |
- Send a Message to a Device                                          | 81   |

#### 9 Device Provisioning Operations

- Automatic Provisioning Operations                                   | 84   |
  - Add an Automatic Provisioning Profile                             | 84   |
  - Edit an Automatic Provisioning Profile                           | 85   |
  - Edit the Profile Order for an Automatic Provisioning Profile      | 85   |
  - Clone an Automatic Provisioning Profile                          | 85   |
  - Delete an Automatic Provisioning Profile                         | 86   |
- Scheduled Provisioning Operations                                  | 86   |
  - View the Scheduled Device Provisioning List and Details          | 86   |
  - Add a Scheduled Provisioning Profile                             | 86   |
  - Edit a Scheduled Provisioning Profile                            | 87   |
  - Clone a Scheduled Provisioning Profile                           | 87   |
  - Delete a Scheduled Provisioning Profile                          | 87   |
  - Schedule a Device for Provisioning                               | 88   |
10 Device Softupdate Operations

Automatic Softupdate Operations ........................................ 91
  View Automatic Softupdate Information .............................. 91
  View Automatic Softupdate Profiles ................................ 92
Implement Automatic Softupdates for Devices ...................... 92
  List the Serial Numbers for the Devices to be Updated ......... 93
Download the Required Software Package ........................... 94
  Request Update Activation Keys .................................... 94
Upload the Software Package and Create a Softupdate Profile ... 95

Scheduled Softupdate Operations ...................................... 96
  View Scheduled Softupdate Information .............................. 96
  View List of Softupdate Profiles .................................... 96
Implement Scheduled Softupdates for Devices ...................... 97
  List the Serial Numbers for the Devices to be Updated ......... 97
Download the Required Software Package ........................... 98
  Request Update Activation Keys .................................... 98
Upload the Software Package and Create a Softupdate Profile ... 99
Schedule the Softupdate for Devices ................................. 100
Cancel Software Updates .............................................. 101

11 Device Details

Device Summary Information ............................................. 103
Device Status Information .............................................. 105
Call Information .......................................................... 107
Device Alerts Information .............................................. 108
Provisioning Details ..................................................... 108
Softupdate Details ........................................................ 109
MCU Device Details .................................................... 110

12 Users and Groups Overview

Groups, Users, and User Roles .......................................... 115
  Local Users ................................................................. 115
  Enterprise Users ......................................................... 116
  Local Groups ............................................................. 117
  Enterprise Groups ....................................................... 118
Roles and Permissions .................................................. 118
Device Associations ...................................................... 121
13 User Management Operations

Manage Users ........................................ 123
Search for a User ................................... 123
Add a User ........................................... 124
Edit a User ......................................... 125
Delete a User ....................................... 126
Manage Groups ..................................... 126
Add a Local Group ................................. 126
Import Enterprise Groups ....................... 127
Edit a Group ....................................... 127
Delete a Group .................................... 128
Manage User Roles ................................. 128
Assign Users Roles and Devices .............. 128

14 System Management Overview

Polycom CMA System Dashboard .............. 131
Dashboard Commands ............................ 134
System Management Menu ..................... 134
System Management Commands .............. 135

15 System Backup and Recovery Operations

Overview of the Polycom CMA System Database .......... 137
Connect to the Polycom CMA System Serial Console .... 138
Backup the Polycom CMA System Database .......... 139
Copy the Polycom CMA System Database Backup Files .... 139
Overview of Database Restoration .................. 141
Restore the Polycom CMA System Internal Databases .... 141
Restore the Polycom CMA System External Database ... 142
Recovery Operations - Reset First Time Setup ........ 142
Restart or Shut Down a Polycom CMA System .......... 143
Disaster Recovery - Restore to Factory Default Image .... 144

16 Directory Setup Operations

Global Address Book ............................... 145
View the Global Address Book .................... 147
Add a User to the Global Address Book .......... 147
Edit a Global Address Book User ............... 148
Delete a Global Address Book User ............. 148
Edit the Global Address Book Password ......... 149
17 Conference Setup Overview
   Conference Templates ................................................. 153
   Conference Settings ............................................... 159

18 Conference Setup Operations
   View the Conference Templates List .............................. 161
   Add a Conference Template ....................................... 161
   Edit a Conference Template ...................................... 162
   Delete a Conference Template .................................. 162
   Set Conference Settings .......................................... 163
   Disable Conference Auto-Launch .................................. 163
   Disable Conference Time Warning ............................... 163
   Edit the Polycom CMA System Email Account ................. 163

19 System Reports
   Gatekeeper Message Log .......................................... 165
      View and Export the Gatekeeper Message Log ............ 167
      Define Log Settings ............................................ 167
      Clear Events from the Log .................................. 167
      Pause and Restart Logging .................................. 168
   Site Statistics .................................................... 168
   Site Link Statistics ............................................... 169
   Call Detail Record Reports ......................................... 169
   Conference Summary Reports .................................... 172
   System Log Files .................................................. 174
      View and Export System Log Files ....................... 176
      Change the System Log Level ............................... 176

20 System Setup Overview
   System Setup Menu ................................................ 179
   Overview of Site Topology ....................................... 180
   Site Topology and Site Link Examples ......................... 182
   Default Polycom CMA System Dial Plan Settings .......... 184
      Site Settings .................................................. 185
      Site Link Settings .......................................... 187
   Polycom CMA System LDAP Integration ........................ 187
   Gatekeeper Overview ............................................. 188
21 Server Setting Operations

Edit the Polycom CMA System Network Settings
Edit the Polycom CMA System Time Settings
Integrate the Polycom CMA System to an External Database
Revert the Polycom CMA System to the Internal Database
Integrate the Polycom CMA System to an Enterprise Server
Enable an Active Directory Domain Controller
Add Polycom CMA System Licenses
Request a Software Activation Key
Enter the Polycom CMA System License Number
Reclaim Polycom CMA Desktop Licenses
Implement a Redundant Polycom CMA 5000 System
Failover to a Redundant Polycom CMA 5000 System Server
Discontinue a Redundant CMA 5000 System Configuration
Add Your Own Logo to the Polycom CMA System User Interface
Add Your Own Logo to the Polycom CMA Desktop User Interface

22 Gatekeeper Management Operations

Primary Gatekeeper Management Operations
Alternate Gatekeeper Management Operations
Neighboring Gatekeeper Management Operations

23 Management & Security Operations

Edit Security Settings to Implement HTTPS
Generate a Certificate Request
Upload a Private Key
Upload a Certificate
Edit the HTTPS Security Setting
Revert to the Default Key and Certificate
Configure Client Systems to Accept HTTPS Certificate
Automatic Endpoint Discovery
Set Common Passwords for Endpoints
Update the Polycom CMA Server Software

24 Dial Plan Setup Operations

Site and Site Link Operations
View the Sites List
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Site</td>
<td>220</td>
</tr>
<tr>
<td>Edit Site Settings</td>
<td>227</td>
</tr>
<tr>
<td>Delete a Site</td>
<td>227</td>
</tr>
<tr>
<td>Site Link Operations</td>
<td>228</td>
</tr>
<tr>
<td>View the Site Links List</td>
<td>229</td>
</tr>
<tr>
<td>Add a Site Link</td>
<td>230</td>
</tr>
<tr>
<td>Edit a Site Link</td>
<td>230</td>
</tr>
<tr>
<td>Delete a Site Link</td>
<td>231</td>
</tr>
<tr>
<td>Gatekeeper Operations</td>
<td>231</td>
</tr>
<tr>
<td>View Neighboring Gatekeeper</td>
<td>232</td>
</tr>
<tr>
<td>Add a Neighboring Gatekeeper</td>
<td>232</td>
</tr>
<tr>
<td>Edit a Neighboring Gatekeeper</td>
<td>233</td>
</tr>
<tr>
<td>Delete a Neighboring Gatekeeper</td>
<td>233</td>
</tr>
<tr>
<td>Dial Plan Service Operations</td>
<td>234</td>
</tr>
<tr>
<td>View the Services List</td>
<td>238</td>
</tr>
<tr>
<td>Add a Service</td>
<td>239</td>
</tr>
<tr>
<td>Edit a Service</td>
<td>240</td>
</tr>
<tr>
<td>Delete a Service</td>
<td>240</td>
</tr>
<tr>
<td>Dial Rule Operations</td>
<td>240</td>
</tr>
<tr>
<td>Pattern Types</td>
<td>243</td>
</tr>
<tr>
<td>Routing Actions</td>
<td>244</td>
</tr>
<tr>
<td>View the Dial Rules List</td>
<td>245</td>
</tr>
<tr>
<td>Add a Dial Rule</td>
<td>246</td>
</tr>
<tr>
<td>Enable or Disable Dialing Rules</td>
<td>247</td>
</tr>
<tr>
<td>Edit a Dial Rule</td>
<td>247</td>
</tr>
<tr>
<td>Least-Cost Routing Operations</td>
<td>248</td>
</tr>
<tr>
<td>LCR Tables for Three Sites</td>
<td>249</td>
</tr>
<tr>
<td>Call Scenario One</td>
<td>251</td>
</tr>
<tr>
<td>Call Scenario Two</td>
<td>251</td>
</tr>
<tr>
<td>View the Least Cost Routing Tables List</td>
<td>252</td>
</tr>
<tr>
<td>Add a Least Cost Routing Table</td>
<td>253</td>
</tr>
<tr>
<td>Edit a Least Cost Routing Table</td>
<td>253</td>
</tr>
<tr>
<td>Delete a Least Cost Routing Table</td>
<td>253</td>
</tr>
</tbody>
</table>

### A  Glossary

### B  System Troubleshooting

- Registration Problems and Solutions ......................... 267
- Point-to-Point Calling Problems and Solutions ............. 270
- MCU and Gateway Dialing Problems and Solutions .......... 271
Conference On Demand Problems and Solutions .......................... 272
Gatekeeper Cause Codes ......................................................... 272

C  System Security and Port Usage
Port Usage ................................................................. 275

D  System Field Input Requirements

Index ................................................................. 287
Polycom® CMA™ System Overview

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

- Features and Capabilities
- Minimum System Requirements
- Other Requirements
- Log Into the Polycom CMA System
- Log Out of the Polycom CMA System
- Working in the Polycom CMA System
  - Polycom CMA Site Map
  - Polycom CMA System Views, Roles, and Permissions
  - Field Input Requirements
  - Filter and Search a List
- Managing Bandwidth

Features and Capabilities

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

- Support for high definition video, voice, and content
- Conference scheduling via the Polycom CMA web scheduling client or the optional Polycom Scheduling Plugins for Microsoft® Outlook® or IBM® Lotus® Notes®
- On-demand conferencing for video endpoint system users
- Automatic or scheduled device provisioning
- Automatic or scheduled device software updates
- Presence, contact list, and chat/instant messaging capabilities
• Access to global user and room directories for on-demand and scheduled calls. Directory service include
  – Global Address Book
  – H.350 and enterprise directory support
    H.350 defines a directory services architecture for multimedia conferencing for H.323, H.320, SIP and generic protocols.
    Currently, the Polycom CMA system supports only a Microsoft Active Directory implementation of an LDAP directory.

• Device monitoring and management
• Conference monitoring and management
• An optional high-availability, redundant management server 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.

**Other Requirements**

Any scheduled call that requires an external MCU requires a Polycom MGC™ or Polycom RMX 2000™ conference platform. The Conference on Demand service also requires a Polycom MGC or RMX 2000 conferencing platform. The Conference on Demand service is not supported on RMX 1000.

**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® 2.0x, or Apple Safari 3.x
• Adobe® Flash® Player 9.x
• The IP address or host name of the Polycom CMA system server and your username, password, and domain.
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 “Configure Client Systems to Accept HTTPS Certificate” on page 215.)

2. When the Polycom CMA system login 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 screens and functions available to your roles. If you log in as an administrator, you see the Polycom CMA system management **Dashboard**.

![Figure 1-1 Polycom CMA System Management Dashboard](image)

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

Polycom CMA 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 screens 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 Schedule Conf View is displayed. They can schedule, monitor, and manage their own conferences. They can also manage the system Guest Book. They cannot perform any other Device, User, System Management, or System Setup tasks, and they cannot monitor or manage 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, Device, User, and System Management menus and the Monitor Conf View is displayed. They can monitor and manage all Polycom CMA system conferences; monitor all devices; manage the system Guest Book; and view reports. They cannot perform any other Device, User, System Management, or System Setup tasks.

- When users who are assigned the default Administrator role log into the Polycom CMA system, they see the Device, User, System Management, and System Setup 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:

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings.</strong> Displays a Settings dialog box with the following information:</td>
</tr>
<tr>
<td>• User Name</td>
</tr>
<tr>
<td>• Remote Server</td>
</tr>
<tr>
<td>• Software Version</td>
</tr>
</tbody>
</table>

In this dialog box, the user can also change the font size used in their display of the Polycom CMA web client interface.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Downloads.</strong> Displays the Downloads dialog box with the downloadable applications compatible with the Polycom CMA system. Downloadable applications include:</td>
</tr>
<tr>
<td>• Polycom CMA Desktop client (including the path to the application)</td>
</tr>
<tr>
<td>• Scheduling Plugin for Microsoft Outlook</td>
</tr>
<tr>
<td>• Scheduling Plugin for IBM Lotus Notes</td>
</tr>
</tbody>
</table>
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 279.

Filter and Search a List

In the Polycom CMA system interface, information is often summarized in a list, for example the Conference List or Participant List.

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 wherever it occurs (beginning, middle, or end) in the word or number.

However, some Polycom CMA system searches—specifically those searches for users in the LDAP 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*
*ar*ar*

But none of the following searches will find Barbara Smithe:

Barb
Smith
*Smi

**Note**

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

---

**Managing Bandwidth**

The Polycom CMA system is responsible for managing bandwidth for calls that it schedules within the gatekeeper region it services. You can create bandwidth management policies by setting the following values:

- **The bandwidth between sites.** The link type and bandwidth are parameters of the site links between two sites. Set it by editing the 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.

- **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.
— 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 management mode devices, 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 link.
This chapter describes the configuration tasks that may be required, based upon 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 Redundancy
- License the Polycom CMA System
- Configure the Connection to the External Database
- Configure the Connection to an External Enterprise Directory
- 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 to respond to DNS queries for the Polycom CMA system by the host name and/or IP address assigned on the System Setup page. The DNS server should also have entries for your Active Directory server (if different from the DNS server) and for the external database server being used by the Polycom CMA system.
To implement the dynamic management mode features of 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 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. This section describes how to complete the configuration of these newly installed redundant servers. It includes these topics:

- Configure the External Database for Redundancy
- Set the Virtual IP Address for the Redundant System

### 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 **System Management > Dashboard > Shutdown** to shut it down.
3. When the primary server has shutdown completely, on the redundant server:
   a. Go to **System Setup > Server Settings > Database**.
   b. On the **Database** screen, 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.

---

*Note*

This procedure describes implementing a new redundant Polycom CMA system. For information on converting an existing system to a redundant system, see “Implement a Redundant Polycom CMA 5000 System” on page 203.
Run the Remote Database Setup Utility and complete the information requested in the setup screens.

- 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.

After the redundant server reboots completely, log into it again and select System Management > Dashboard > Shutdown to shut it down.

When the redundant server has shutdown completely, on the primary server:

- Turn ON the primary server.
- Log into the server and go to System Setup > Server Settings > Database.
- On the Database screen, select the Use an external SQL Server database check box.
- 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).
- Click Update.

The primary server reboots and comes online as the primary server.

When the primary server has rebooted 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 System Setup > 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 screen.

3. Enter the Virtual IP for the redundant system and click Submit. For information about this virtual IP address, see “Implement a Redundant Polycom CMA 5000 System” on page 203.

Note
Set the virtual IP for the redundant server on the primary server only.
License the Polycom CMA System

To license a non-redundant Polycom CMA system, see “Add Polycom CMA System Licenses” on page 201. 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” on page 202.

2. On the primary Polycom CMA 5000 system server:
   a. Go to System Setup > 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 System Setup > Server Setup > 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 System Setup > 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 System Setup > Server Setup > Licenses.
   b. Enter the software activation key code for the redundant server into the Activation Key field and click Add.
   c. Go to System Management > Dashboard > Restart to reboot the system.
      The system fails over to the primary server.
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 198.

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. We recommend implementing an external database if your Polycom CMA 4000 system has 100+ registered endpoints.

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 Server” on page 199.

Connecting to an enterprise directory allows users to enter their standard 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.

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 Operations” on page 219.

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 84.
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 Devices” on page 92.

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 Conference 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 153.

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 or Global Directory Server (GDS) to point to the Polycom CMA system IP address or DNS name. Use the same 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 screens and fill in missing information.

   You can also register endpoints to the directory from the Directory Setup screens. 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 “Device Management Overview” on page 51.

2 Set up users and associate them with devices. Unless your Polycom CMA system is integrated with an enterprise directory, you must enter all user information manually including device 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 directory users with devices. For more information, see “Directory Setup Operations” on page 145.

3 Set up groups, add members, and associate them with provisioning profiles. For more information, see “Directory Setup Operations” on page 145.

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 “Directory Setup Operations” on page 145.

**Distribute Polycom Applications**

After you’ve installed the Polycom CMA system, you can distribute the Polycom CMA Desktop client application to users.

**Note**

You can brand the Polycom CMA Desktop client with your company logo or a design of your choice. See the *Polycom CMA System Operations Guide*.

To deploy the Polycom CMA Desktop client, 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 `.msi` or `.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.
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 the 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 to be sent to users. Edit the following sample instructions (the procedure encased by the dashed lines) for your situation.

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. 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.

You’re now ready to connect to anyone else using Polycom CMA Desktop or other types of video conferencing 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 the 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 to be sent to users. Edit the following sample instructions (the procedure encased by the dashed lines) for your situation.

To install the 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.
   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.

10. Click Sign In.
    You’re now ready to connect to anyone else using Polycom CMA Desktop or other types of video conferencing systems.

11. 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.
   You’re now ready to connect to anyone else using Polycom CMA Desktop or other types of video conferencing systems.
Conference Scheduling Overview

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

- Schedule Conference View
- Monitor Conf View
- Conference Commands

## Schedule Conference View

Use the **Schedule Conf View** to view and edit future conferences. The **Schedule Conf View** has these sections.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>The context-sensitive set of available commands</td>
</tr>
<tr>
<td>Conference List</td>
<td>By default the conference list in the <strong>Schedule Conf View</strong> displays <strong>Future Only</strong> conferences, while the conference list in the <strong>Monitor Conf View</strong> displays <strong>Ongoing Plus</strong> conferences. Filter choices include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Future Only</strong> - Displays scheduled conferences that have not yet started</td>
</tr>
<tr>
<td></td>
<td>• <strong>Today Only</strong> - Displays scheduled conferences (completed, active, or future) for the current day and active ad hoc conferences</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom Date</strong> - Displays scheduled conferences (completed, active, or future) for a selected day. Select the day from the calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Ongoing Plus</strong> - Displays ongoing and future conferences for the day. You can further filter this request by <strong>Conference Name</strong>.</td>
</tr>
</tbody>
</table>
### Section | Description
--- | ---

**Conference List (continued)** | • **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 **Conference Name**.
• **Yesterday Plus** - Displays completed scheduled conferences for yesterday and earlier. You can further filter this request by **Conference Name**.

For information on filters, see “Filter and Search a List” on page 6.

**Conference Details** | Displays information about the conference selected in the **Conference List** including:
• Conference Features
• Bridge (MCU) Features
• Participant Details

**Conference Features** | Displays the status of the Polycom CMA system features for the selected conference

**Bridge (MCU) Features** | Displays the status of MCU features for the selected conference

**Conference Notes** | Displays any notes you added to the conference email notification for the selected conference

**Participants** | Displays the list of participants for the selected conference

**Participant Details** | Displays information about the participant selected in the **Participants** list

---

**Monitor Conf View**

Use the **Monitor Conf View**, available from the **Conference** menu, to monitor and manage ongoing conferences. The **Monitor Conf View** has the same sections as the **Schedule Conf View** but with the **Ongoing Plus** filter applied.
Conference Commands

Access these commands from the Conference menu and the Commands section of both the Schedule Conf View and Monitor Conf View.

<table>
<thead>
<tr>
<th>Command</th>
<th>When selected...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Conf View</td>
<td>Displays the Conference List - Schedule View in the main window. Use this view to work with future conferences.</td>
</tr>
<tr>
<td>Monitor Conf View</td>
<td>Displays the Conference List - Monitor View in the main window. Use this view to work with active conferences.</td>
</tr>
<tr>
<td>Refresh View</td>
<td>Updates the display with current information</td>
</tr>
<tr>
<td>Add Conference</td>
<td>Displays the Add Conference screen. Use this link to create a new audio and/or video conference</td>
</tr>
</tbody>
</table>

**Note**

By default the Schedule Conf View displays future conferences while the Monitor Conf View displays ongoing and future conferences for the day. You can use the Filter to customize views. For information on filters, see “Filter and Search a List” on page 6.

The Commands section may also include these other context-sensitive commands depending on the type of conference selected.

**Table 3-1  Context-sensitive Conference Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available for future conferences</td>
<td></td>
</tr>
<tr>
<td>Edit Conference</td>
<td>Displays the Edit Conference screen for the conference selected in the Conference List. Use this command to edit the selected future conference. For information, see “Edit a Conference” on page 30.</td>
</tr>
<tr>
<td>Delete Conference</td>
<td>Deletes the conference selected in the Conference List. Use this command to delete the selected past or future conference. For information, see “Delete a Conference” on page 29.</td>
</tr>
</tbody>
</table>
Table 3-1  Context-sensitive Conference Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available for active conferences</td>
<td></td>
</tr>
<tr>
<td>Manage Conference</td>
<td>Displays the Manage Conference screen for the conference selected in the Conference List. Use this command to manage participants and devices in the selected active conference. For information, see “Manage an Active Conference” on page 33.</td>
</tr>
<tr>
<td>Terminate Conference</td>
<td>Ends the selected conference. For information, see “Manage an Active Conference” on page 33.</td>
</tr>
</tbody>
</table>
This chapter describes the Polycom® Converged Management Application™ (CMA™) system conference management operations. It includes these topics:

- Add a Conference
- Delete a Conference
- Edit a Conference
- Edit a Participant’s Settings
- Edit a Room’s Settings
- Manage an Active Conference
- Manage a Participant Device During a Conference

### Add a Conference

**To add a new conference:**

1. Go to Conference > Add Conference.
2. In the Add Conference screen, 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 an **Audio Only** conference:

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

The drop-down selections change to **Default Audio Template** and **Any MGC**. Your selection may also include individual MGC devices defined to the Polycom CMA system. Also, the system automatically identifies the conference as a dial-in conference that requires MCU resources.

b To select a template other than the default, click **Default Audio Template** and select a different template.

Depending on your template selection, the **Any MGC** selection may change to **Any MCU** or **Any RMX** to extend your selection to RMX devices. Your selection may also include individual RMX and MGC devices defined to the Polycom CMA system.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any MGC</td>
<td>The template indicates that the conference requires an MGC, but the system may select which MGC to use</td>
</tr>
<tr>
<td>Any MCU</td>
<td>The template indicates that the conference requires an MCU, but the system may select which MCU to use</td>
</tr>
<tr>
<td>Any RMX</td>
<td>The template indicates that the conference requires an RMX, but the system may select which MGC to use</td>
</tr>
</tbody>
</table>

c To select a specific MCU to host the conference, select the MCU from the MCU list.

5 For a **Video** conference:

a To select a template other than the default, click **Default Template** and select a different template.

Depending on your template selection, the **Auto MCU Selection** may change to **Any MCU**, **Any MGC**, or **Any RMX**, and the MCU list may also include individual RMX and MGC devices defined to the Polycom CMA system.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto MCU Selection</td>
<td>The template does not require an MCU, but the system may use MCU resources if needed</td>
</tr>
<tr>
<td>Any MCU</td>
<td>The template indicates that the conference requires an MCU, but the system may select which MCU to use</td>
</tr>
</tbody>
</table>
To select a specific MCU to host the conference, select the MCU from the MCU list.

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’s names that meet your search criteria.

   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 From the Add From Guest Book dialog box, select the guest to add to the conference and click Close.

   The guests’ name appears in the underlying Selected Participants and Rooms list.

   c 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 and Email address. Note that the Email address field is ASCII only. For more information, see “Field Input Requirements” on page 6.
c Select how the guest will join the conference.

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

e For a guest with a video endpoint system, set the **Bit Rate** and **Dial Options** settings as required. (You can change the connection speed for an endpoint up to the maximum speed set by the conference template.)

f If you select **Dial Out**, enter the guest’s number in the **Number** field.

g Click **OK and SAVE** to add the guest and save the guest’s information to the **Guest Book** or click **OK** to simply add the guest.

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.

b Edit participant dial settings as needed by selecting the participant and clicking **Edit**. See step 4 on page 31.

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

a Click **Select Site**.

b Select the site from the site list

The conference room list for the selected site appears.

c Select a conference room 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**.

---

**Notes**

- For participants who are associated with devices, the Polycom CMA system schedules their availability according to their device availability.
- For participants with multiple devices, you must check the availability for each device. The **Add Conference** dialog box provides a participant device list to do this.
Once you’ve added your participants, you can assign them leadership roles or edit their call settings:

a. To assign an invitee as lecturer, in the Lecturer field select the participant’s name from the list.

b. To assign an invitee as video chairperson, in the Video Chairperson field select the participant’s name from the list.

c. To edit a participant’s dial settings, select the participant from the Selected Participants and Rooms list, click Edit for the participant, and edit the settings as necessary.

When finished, click Schedule.

The Conference Email Notification screen appears with a message indicating Conference Successfully Scheduled.

To exit without sending an email to your invitees, click Skip Email.

To send an email notification to your invitees, in the Conference Email Notification screen:

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.

Delete a Conference

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

To delete a conference

1. Go to Conference > Schedule Conf View.

2. To delete a past conference, select the appropriate filter (such as Yesterday Plus).
3 From the **Conference List**, select the conference of interest and click **Delete Conference**.

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.

4 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.

---

**Edit a Conference**

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

**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.

**To edit a future conference**

1 Go to **Conference > Schedule Conf View**.

2 From the **Conference List**, select the conference of interest and click **Edit Conference**.

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 required choice and click **Edit**.

   The **Edit Conference** window appears. Except for the title, it is just like the **Add Conference** screen.

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

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 25.

6 When finished, click **Schedule**.

   The **Conference Email Notification** screen appears with a message indicating **Conference Successfully Scheduled**.
7 To exit without sending an updated email to your invitees, click **Skip Email**.

8 To send an updated email to your invitees, in the **Conference Email Notification** screen:
   - Copy additional people on the notification and/or add notes about the conference.
   - Click **Send**.

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

   The Polycom CMA system changes required resources as needed.

   The **Conference List - Schedule View** appears.

---

**Edit a Participant’s Settings**

You can edit a participant’s call settings for future scheduled conferences. You cannot edit a participant’s call settings for an active conference.

**To edit a participant’s settings**

1 Go to **Conference > Schedule Conf View**.

2 From the **Conference List**, select the conference of interest and click **Edit Conference**.

   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 required choice and click **Edit**.

3 In the **Edit Conference** screen, select the participant of interest from the **Selected Participants and Rooms** list and click **Edit**.

4 Configure these settings in the **Edit Participant Settings** dialog box as required.
   - The participant’s endpoint, if the participant has more than one available
   - Select how the participant will join the conference.

     Audio-only participants are required to dial into the conference. For a participant joining the conference using a video device, you have two options:

     » To require that the participant dial into the conference and enter a PIN code, select the **Dial-In** setting.
     » To bring the participant into the conference by dialing out to the participant, use the **Dial-Out** setting.
— For participants with audio endpoints, set the Dial Type setting to IP or ISDN as required.

— For participants with video endpoint systems, set the Bit Rate and Dial Options settings. (You can change the connection speed for an endpoint up to the maximum speed set by the conference template.)

— If you select Dial Out, enter the participant’s number.

5 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 > Schedule Conf View.

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 required choice and click Edit.

4 In the Edit Conference screen, select the room of interest from the Selected Participants and Rooms list and click Edit.

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

   — The room’s endpoint, if the room has more than one available
   — Select how the room will connect to the conference.
   — For rooms with audio endpoints, set the Dial Type setting to IP or ISDN as required.
   — For rooms with video endpoint systems, set the Bit Rate and Dial Options settings. (You can change the connection speed for an endpoint up to the maximum speed set by the conference template.)
   — If you select Dial Out, enter the number for the room’s endpoint in the Number field.

6 Click OK.
Manage an Active Conference

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

To manage an active conference

1. Go to Conference > Monitor Conf View.

2. From the Conference List, select the active conference of interest and click Manage.

   The Manage Conference screen appears displaying the Participants list.

3. To end the conference:
   a. Click Terminate Conference.
   b. Click Terminate to confirm the termination.

4. To extend the conference:
   a. Click Extend Conference.
   b. From the Extend Conference dialog box, click the time menu and select the number of minutes by which to extend the conference.
   c. Click Update.

5. To add additional conference participants from your 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’s names that meet your search criteria.

   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.

   d. If necessary, edit the new participants’ dial settings. See “Edit a Participant’s Settings” on page 31.

Notes

- Depending on the search domain, the search function may return different results. See “Filter and Search a List” on page 6.
- The search results only include users associated with devices.
6 To add a guest from the Guest Book:
   a Click Add From Guest Book.
   b From the Add From Guest Book dialog box, select the guest to add to the conference and click Close.
      The guests’ name appears in the underlying Selected Participants and Rooms list.
   c Click Close.

7 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 and Email address. Note that the Email address field is ASCII only. For more information, see “Field Input Requirements” on page 6.
   c Select how the guest will join the conference.
   d For guests with audio endpoints, set the Dial Type setting to IP or ISDN as required.
   e For guests with video endpoint systems, set the Bit Rate and Dial Options settings as required. (You can change the connection speed for an endpoint up to the maximum speed set by the conference template.)
   f If you select Dial Out, enter the guest’s number in the Number field.
   g Click OK and SAVE to add the guest and save the guest’s information to the Guest Book or click OK to simply add the guest.
      The guest’s name appears in the underlying Selected Participants and Rooms list.
   h If necessary, edit the new participants’ dial settings. See “Edit a Participant’s Settings” on page 31.

8 To dial out to the new participants or guests, select them from the list and click Connect New Participants.

9 To change the layout for the conference:
   a Click Change Layout.
b From the Choose Video Mode dialog box, select the desired conference layout. For more information about video mode, see “Edit Advanced Conference Settings” on page 40.

c Click Update.

Manage a Participant Device During a Conference

The Manage Conference screen (Figure 2-2 on page 13) also allows you to manage conference participant’s endpoints. Essentially, you become the conference moderator.

From the Participant List on the Manage Conference screen, you may use these context-sensitive commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mute/Unmute participant</td>
<td>To mute and unmute the sound to a conference for a registered participant. The audio icon shows the current status of this setting. This icon appears only when the conference is running on an external MCU</td>
</tr>
<tr>
<td>Connect/Disconnect participant</td>
<td>To disconnect and reconnect the device associated with a participant. Disconnected participants and their devices are still associated with the conference and are not available for other conferences.</td>
</tr>
<tr>
<td>Remove participant</td>
<td>To remove a participant from the conference participant list at which time the participant becomes available for another conference</td>
</tr>
<tr>
<td>Send message</td>
<td>(Users with administrator or operator permissions only) To send a message to a participant’s registered Polycom endpoints. The message appears briefly on the monitor for the selected video endpoint system.</td>
</tr>
<tr>
<td>Acknowledge help</td>
<td>(Users with administrator or operator permissions only) To acknowledge a request for help and send a message to the requesting endpoint</td>
</tr>
</tbody>
</table>

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 > Monitor Conf View.
2 From the **Conference List**, select a conference to manage and click **Manage**.

The **Manage Conference** screen appears (Figure 2-2 on page 14) displaying the **Participants** list.

3 To mute or unmute a participant’s endpoint:
   a Select the participant of interest from the **Participant** list.
   b Click the **Mute Participant** or **Unmute Participant**, depending on the participant’s current state.

   The participant’s state changes.

4 To connect or disconnect a participant:
   a Select the participant of interest from the **Participant** list.
   b Click **Connect Participant** or **Disconnect Participant**, depending on the participant’s current state.

   The participant’s state changes.

5 To remove a participant from the conference:
   a Select the participant of interest from the **Participant** list and click **Remove Participant**.
   b Click **Remove** to confirm the removal.

6 To send a message to a participant’s endpoint:
   a Select the participant of interest from the **Participant** list and click **Send Message**.
   b In the **Send Message** dialog box, type the message.
   c Click **Send**.

   The message is sent to the endpoint’s screen.

7 To acknowledge a participant’s request for help:
   a Select the participant of interest from the **Participant** list and click **Acknowledge Help**.
   b In the **Send Message** dialog box, type a message that acknowledges the help request.
   c Click **Send**.

   The message is sent to the endpoint’s screen.
   d Click **Close**.
This chapter describes how a user with advanced scheduler permissions can edit some conference settings for conferences scheduled through the Polycom® Converged Management Application™ (CMA™) system.

### Advanced Conference Settings

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 MGC and RMX 2000 devices), and the conference you schedule lands on the RMX 2000 platform, some of the settings you specify here may be overridden by the RMX profile. See Table 5-1.

**Notes**

- A profile is a collection of advanced conference settings that reside on the MCU (MGC or RMX). Only an RMX profile can override conference template settings. For more information about conference templates, profiles, and your conferencing configuration, contact your Polycom CMA system administrator.
- 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Password</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 an RMX 2000 MCU 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.
- 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.

Dial Options You have three options:
- To create a conference for which dial information and a PIN code are assigned to all conference participants, use the Dial-In setting. This setting allows any audio or video endpoint system to dial in, and all participants can 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 endpoint systems 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 screen layout on an 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 screen, 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.

### Table 5-1  Advanced Conference Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. **Notes**
|                     | • If a conference is scheduled on an RMX 2000 MCU 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. **Notes**
|                     | • RMX 1000 systems do not support the Chairperson feature. **Notes**
| Chairperson Password| If Enable Chairperson is selected, the chairperson must enter this four-digit password at their endpoint to assume control. **Notes**
|                     | The system sends a separate email with this password to the video chairperson. It is not included in the conference notification email. **Notes**
| Dial Options        | You have three options: **Notes**
|                     | • To create a conference for which dial information and a PIN code are assigned to all conference participants, use the Dial-In setting. This setting allows any audio or video endpoint system to dial in, and all participants can connect to the same conference on the MCU. **Notes**
|                     | • To dial out to all participants in the conference, use the Dial-Out setting. **Notes**
|                     | • To allow participants both options, select Dial-In+Dial-Out. **Notes**
|                     | **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. **Notes**
| Always Use MCU      | This setting forces the conference to an MCU and prevents video endpoint systems 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. **Notes**
| Video Mode          | Determines the initial screen layout on an endpoint's monitor for a multipoint conference that requires an MCU. The options are: **Notes**
|                     | • Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. **Notes**
|                     | • Continuous Presence. Displays several panels on the screen, 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. **Notes**
|                     | • Automatic Layout is a continuous presence layout, in which the number of participants determines the number of panels. **Notes**
Table 5-1  Advanced Conference Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 device. 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.  

---

Table 5-1  Advanced Conference Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
Edit Advanced Conference Settings

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

To edit the conference settings

1. When you add a conference or edit a scheduled conference, on the Conference Resources tab, click Edit Conference Settings.

2. As required, edit the conference settings. The settings that you can edit depend on the template selected.

3. Click OK.

Table 5-1  Advanced Conference Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| T.120 Mode      | Selects the protocols and specifications for multipoint data communication. From 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. |
This chapter lists the conference and participant field names and descriptions for reference. It includes these topics:

- Conference List
- Conference Details
- Conference Features
- Bridge (MCU) Features
- Participants
- Participant Details
- Participant Settings
- Participant Settings

### Conference List

The **Conference List** has these fields.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The state of the conference. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Conference ending</td>
</tr>
<tr>
<td></td>
<td>• Active</td>
</tr>
<tr>
<td></td>
<td>• Active with alerts</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Declined</td>
</tr>
<tr>
<td></td>
<td>• Future</td>
</tr>
</tbody>
</table>
Conference Details

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

### Table 6-1  Fields of the Conference List

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of conference. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Audio Only</td>
</tr>
<tr>
<td></td>
<td>• Video</td>
</tr>
<tr>
<td></td>
<td>• Recurring</td>
</tr>
<tr>
<td>Conference Name</td>
<td>The name assigned to the conference when it was created</td>
</tr>
<tr>
<td>Start Time</td>
<td>For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time.</td>
</tr>
<tr>
<td></td>
<td>For an unscheduled conference, the date and time the conference started.</td>
</tr>
<tr>
<td>Owner</td>
<td>The name of the person who created the conference. As a scheduler, you only see the conferences you own.</td>
</tr>
<tr>
<td>Actions</td>
<td>The actions you can perform on the conference. Possible buttons include:</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Edit</td>
</tr>
<tr>
<td></td>
<td>• Manage</td>
</tr>
</tbody>
</table>

### Table 6-2  Fields of the Conference Details section

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>The name of the person who created the conference. Schedulers only see the conferences they own.</td>
</tr>
<tr>
<td></td>
<td>Not applicable for ad hoc conferences.</td>
</tr>
<tr>
<td>Start Date/Time</td>
<td>For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time.</td>
</tr>
<tr>
<td></td>
<td>For an unscheduled conference, the date and time the conference started.</td>
</tr>
<tr>
<td>Duration</td>
<td>For a scheduled conference, how long the conference is scheduled to last.</td>
</tr>
<tr>
<td></td>
<td>For a completed conference, how long the conference actually lasted.</td>
</tr>
<tr>
<td>End Date/Time</td>
<td>The date and time the conference ended</td>
</tr>
</tbody>
</table>
### Table 6-2  Fields of the Conference Details section

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

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

**Table 6-2**  
**Fields of the Conference Details section**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Algorithm</td>
<td>For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• AUTO</td>
</tr>
<tr>
<td></td>
<td>• G.711</td>
</tr>
<tr>
<td></td>
<td>• G.722</td>
</tr>
<tr>
<td></td>
<td>• Siren 7 (16 kbps)</td>
</tr>
<tr>
<td></td>
<td>• Siren 14 (24 kbps)</td>
</tr>
<tr>
<td></td>
<td>• Siren 14 (32 kbps)</td>
</tr>
<tr>
<td></td>
<td>• Siren 14 (48 kbps)</td>
</tr>
<tr>
<td></td>
<td>See the device documentation for more information.</td>
</tr>
</tbody>
</table>

**Table 6-3**  
**Fields of the Conference Features section**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Password</td>
<td>The conference password, which is assigned either by the system or the scheduler</td>
</tr>
<tr>
<td>Chairperson Required</td>
<td>Whether or not the conference requires a chairperson</td>
</tr>
<tr>
<td>Note</td>
<td>The RMX 1000 system does not support the Chairperson feature.</td>
</tr>
<tr>
<td>Chairperson Password</td>
<td>The password the chairperson must enter. Not applicable when no chairperson is designated.</td>
</tr>
<tr>
<td>Chairperson</td>
<td>The name of the chairperson. Not applicable when no chairperson is designated.</td>
</tr>
<tr>
<td>Lecture Mode</td>
<td>The type of Lecture Mode, if any, that was selected when the conference was created. Possible values are:</td>
</tr>
<tr>
<td>Note</td>
<td>The RMX 1000 system does not support Lecture Mode.</td>
</tr>
<tr>
<td>Lecturer</td>
<td>The name of the lecturer. Not applicable when Lecture Mode is None.</td>
</tr>
<tr>
<td>Lecture View Switching</td>
<td>Indicates whether or not automatic switching between participants is enabled.</td>
</tr>
</tbody>
</table>
Table 6-3  Fields of the Conference Features section

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Stream Mode</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• People+Content</td>
</tr>
<tr>
<td></td>
<td>• Duo Video</td>
</tr>
<tr>
<td></td>
<td>• Visual Concert PC</td>
</tr>
<tr>
<td>T120 Rate</td>
<td>Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• HMLP - Var</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 384</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 320</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 256</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 192</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 128</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 6.4</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 62.4</td>
</tr>
<tr>
<td></td>
<td>• HMLP - 14.4</td>
</tr>
<tr>
<td></td>
<td>• MLP - Var</td>
</tr>
<tr>
<td></td>
<td>• MLP - 64.4</td>
</tr>
<tr>
<td>End Time Alert</td>
<td>Whether or not the system alerts participants to the end of the conference</td>
</tr>
<tr>
<td></td>
<td>by playing an end tone</td>
</tr>
<tr>
<td>Entry Tone</td>
<td>Whether or not an entry tone is played to all connected participants when a</td>
</tr>
<tr>
<td></td>
<td>participant joins the conference</td>
</tr>
<tr>
<td>Exit Tone</td>
<td>Whether or not an exit tone is played to all connected participants when a</td>
</tr>
<tr>
<td></td>
<td>participant disconnects from the conference</td>
</tr>
</tbody>
</table>
The **Bridge (MCU) Features** section, which applies only for conferences that use an MCU, has these fields.

### Table 6-4  Fields of the Bridge (MCU) Features section

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCU Name</td>
<td>The MCU device name hosting the conference. Not applicable when the conference is not being hosted on an MCU.</td>
</tr>
<tr>
<td>Numeric ID</td>
<td>The unique conference identifier assigned by the MCU</td>
</tr>
<tr>
<td>Entry Queue Access</td>
<td>Whether or not the conference has an entry queue enabled</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Meet Me per Conf</td>
<td>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</td>
</tr>
<tr>
<td>Conference on Port</td>
<td>(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.</td>
</tr>
<tr>
<td>Message Service Type</td>
<td>Displays the type of messages participants joining the conference hear. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Welcome (No wait)</td>
</tr>
<tr>
<td></td>
<td>• Attended (Wait)</td>
</tr>
<tr>
<td></td>
<td>• IVR</td>
</tr>
<tr>
<td>Message Service Name</td>
<td>Name on the MCU of the Message Service. So, for example, a service name IVR70 which provides the IVR service.</td>
</tr>
</tbody>
</table>
Participants

The **Participants** section has these fields.

<table>
<thead>
<tr>
<th>Table 6-5</th>
<th>Fields of the Participants section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Name</td>
<td>The participant’s name</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Table 6-6</th>
<th>Fields of the Participant Details section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Name</td>
<td>The participant’s name</td>
</tr>
</tbody>
</table>
| Type | The type of conference connection. Possible values include:  
  • Audio Only  
  • Audio-Video  
  • Other (for In Person and Room Only participants) |
| Device Name | The name assigned to the participant’s endpoint when added to the system |
| Connection Status | The state of the participant’s endpoint connection. Possible values include:  
  • Connected  
  • Connecting  
  • Declined  
  • Disconnected  
  • Disconnecting  
  • Error  
  • Unknown |
### Participant Settings

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

#### Table 6-6  Fields of the Participant Details section

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Type</td>
<td>The interface protocol of the participant's endpoint. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• IP</td>
</tr>
<tr>
<td></td>
<td>• ISDN</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address or phone number of the participant's endpoint (if a dial-out) or the participant's port address on the MCU (if a dial-in)</td>
</tr>
<tr>
<td>Bit Rate</td>
<td>The audio or video data transfer rate (in kbps) of the participant's endpoint</td>
</tr>
</tbody>
</table>

#### Table 6-7  Fields of the Participant Settings dialog box

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

**Table 6-7**  
*Fields of the Participant Settings dialog box*

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Rate</td>
<td>The audio or video data transfer rate (in kbps) of the participant’s endpoint</td>
</tr>
</tbody>
</table>
| 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.                       |

*For more information on field limitations, see “Field Input Requirements” on page 1-6.

**Table 6-8**  
*Fields of the Participant Settings dialog box*

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>(H.320 dial type only) The country to which the system will dial out to the participant</td>
</tr>
<tr>
<td>Area/City Code</td>
<td>(H.320 dial type only) The area code to which the system will dial out to the participant</td>
</tr>
<tr>
<td>Number</td>
<td>(H.323 and H.320 dial types) The participant’s phone number</td>
</tr>
<tr>
<td>Use Modified Dial Number</td>
<td>(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</td>
</tr>
<tr>
<td>Number</td>
<td>(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.</td>
</tr>
</tbody>
</table>
**Manage Conference - Participants List**

The *Manage Conference - Participants* list has these fields.

*Table 6-9  Fields of the Manage Conference - Participant list*

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Status       | The state of the participant’s connection. Possible states include:  
  - Connected  
  - Disconnected  
  - 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 |
Device Management Overview

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

- Device Menu, Views, and Lists
- Device Types
- Device Configuration/Provisioning
- Device Softupdates
- Device Passwords

Device Menu, Views, and Lists

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

- Admin/Monitor View
- Automatic Provisioning View
- Scheduled Provisioning View
- Automatic Softupdate View
- Scheduled Softupdate View

Information in the Device Views

All of the device views have the following information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>The context-sensitive set of commands available in the selected view for the selected device</td>
</tr>
<tr>
<td>Device List</td>
<td>The context-sensitive device list for the selected view</td>
</tr>
</tbody>
</table>
When you log into the Polycom CMA system with Operator role and permissions, the Admin/Monitor View appears. Use this view to monitor and manage devices.

Device List in the Admin/Monitor View

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

The Device List has these fields.

Table 7-1 Fields of the Admin/Monitor View Device List

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Filter choices for this view include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong> - Filters the device list by device type. For more information, see “Device Types” on page 61.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alerts</strong> - Filters the device list by device alert type: Help, Error, or Warning</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connection Status</strong> - Filters the device list by device connection status: In a Call, Online, or Offline</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> - Searches the device list by system name</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> - Searches the device list by device IP address</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN Video Number</strong> - Searches the device list by device ISDN video number</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alias</strong> - Searches the device list by device alias</td>
</tr>
<tr>
<td></td>
<td>• <strong>Site</strong> - Searches the device list by device site location</td>
</tr>
<tr>
<td></td>
<td>• <strong>VIP</strong> - Searches the device list for VIP devices</td>
</tr>
</tbody>
</table>
Table 7-1  Fields of the Admin/Monitor View Device List

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The state of the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Online</td>
</tr>
<tr>
<td></td>
<td>• Offline</td>
</tr>
<tr>
<td></td>
<td>• In a call</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• Device alert</td>
</tr>
<tr>
<td></td>
<td>• Gatekeeper registration error</td>
</tr>
<tr>
<td>Mode</td>
<td>The management mode for the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Dynamic management mode</td>
</tr>
<tr>
<td></td>
<td>• Standard management mode (no icon)</td>
</tr>
<tr>
<td></td>
<td>For a description of these modes, see “Device Types” on page 61.</td>
</tr>
<tr>
<td>Name</td>
<td>The system name of the device</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device. For valid device types, see “Device Types” on page 61.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the device</td>
</tr>
<tr>
<td>Alias</td>
<td>The alias to connect to the device</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the device</td>
</tr>
<tr>
<td>Owner</td>
<td>(Endpoints only) The user associated with the device</td>
</tr>
</tbody>
</table>

 Commands in the Admin/Monitor View

Besides providing access to the device views, the Commands section of the device Admin/Monitor View may also include these other context-sensitive commands depending on the selected device type.

Table 7-2  Device Commands - Admin/Monitor View

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Device</td>
<td>Manually add a device to the Polycom CMA system or find a device on the network</td>
</tr>
<tr>
<td>View Device Details</td>
<td>Display all of the Device Details for the selected device</td>
</tr>
<tr>
<td>Edit Device</td>
<td>Change connection settings for the selected device. Note that if this is a managed device, the device may overwrite settings entered manually.</td>
</tr>
</tbody>
</table>
Automatic Provisioning View

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

Device List in the Automatic Provisioning View

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

---

**Table 7-2 Device Commands - Admin/Monitor View (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Delete Device</td>
<td>Delete the selected device or devices. To select devices for this operation, you must click the checkboxes for the device. You can delete multiple devices at one time.</td>
</tr>
<tr>
<td>Available for only selected device types</td>
<td></td>
</tr>
<tr>
<td>Manage Device</td>
<td>Open the selected device's management interface in a separate browser window. This command is not available for the following device types: MGC, GW/MCU, Tandberg, iPower, PVX, and Other.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Send a text message (ASCII only, 100 characters maximum) to the selected device’s video screen. This command is not available for the following device types: MGC, RMX, GW/MCU, Tandberg, iPower, and Other.</td>
</tr>
<tr>
<td>Clear Help</td>
<td>Clear help for the selected device on the Polycom CMA system</td>
</tr>
<tr>
<td>Reboot Device</td>
<td>Reboot the selected device. This command is only available for HDX-Series, V-Series and VSX-Series devices with a Connection Status of Online.</td>
</tr>
<tr>
<td>Manage User</td>
<td>Change information for the selected user. This command is applicable only when the user is associated with a device.</td>
</tr>
</tbody>
</table>

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

For information about these device commands, see “Device Management Operations” on page 71.
The device list in the **Automatic Provisioning View** has the following information.

**Table 7-3  Fields of the Device List in the Automatic Provisioning View**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>The filter choice for this view is device type only. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• HDX-Series—Displays the Polycom HDX systems deployed in dynamic management mode</td>
</tr>
<tr>
<td></td>
<td>• CMA Desktop—Displays the Polycom CMA systems</td>
</tr>
<tr>
<td></td>
<td>• All—Polycom HDX and Polycom CMA Desktop systems together</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the device’s last provisioning process. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Clear</td>
</tr>
<tr>
<td>Name</td>
<td>The system name of the device</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Polycom CMA Desktop systems are assigned a user name of LastName_Firstname_CMADesktop</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device. Automatic provisioning is only available for these device types:</td>
</tr>
<tr>
<td></td>
<td>• HDX-Series—Polycom HDX system devices deployed in dynamic management mode</td>
</tr>
<tr>
<td></td>
<td>• CMA Desktop—Polycom CMA Desktop systems</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the device</td>
</tr>
<tr>
<td>Last</td>
<td>The date and time of the device’s last provisioning</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Polycom CMA Desktop systems are provisioned at the start of each session</td>
</tr>
</tbody>
</table>

**Commands in the Automatic Provisioning View**

Because automatic (pull) provisioning is managed by the device, there are no commands available in the **Automatic Provisioning View**.
Scheduled Provisioning View

Use the Scheduled Provisioning View to:

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

Device List in the Scheduled Provisioning View

By default the device 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 device list in the Scheduled Provisioning View has the following information.

Table 7-4 Fields of the Device List in the Scheduled Provisioning View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>The filter choice for this view is device type only. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• HDX-Series—Displays the Polycom HDX systems operating in standard (non-dynamic) management mode</td>
</tr>
<tr>
<td></td>
<td>• V-Series or VSX-Series</td>
</tr>
<tr>
<td></td>
<td>• Viewstation</td>
</tr>
<tr>
<td></td>
<td>• Viewstation FX &amp; EX</td>
</tr>
<tr>
<td></td>
<td>• Tandberg</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the device’s last provisioning process. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• Clear</td>
</tr>
<tr>
<td>Name</td>
<td>The system name of the device</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device. Scheduled provisioning is only available for these devices types:</td>
</tr>
<tr>
<td></td>
<td>• ViewStation</td>
</tr>
<tr>
<td></td>
<td>• ViewStation FX &amp; EX</td>
</tr>
<tr>
<td></td>
<td>• V-Series or VSX-Series</td>
</tr>
<tr>
<td></td>
<td>• Tandberg MXP Series</td>
</tr>
<tr>
<td></td>
<td>• HDX-Series—Polycom HDX systems operating in standard (non-dynamic) management mode</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the device</td>
</tr>
</tbody>
</table>
Besides providing access to the device views, the Commands section of the device Scheduled Provisioning View also includes these commands:

### Table 7-5 Device Commands - Scheduled Provisioning View

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Device</td>
<td>Manually add a device to the Polycom CMA system</td>
</tr>
<tr>
<td>❑ Provision</td>
<td>Schedule provisioning for the selected device(s). To select devices, you must click the checkbox for the device. You can provision multiple devices of the same type at one time using the same provisioning profile.</td>
</tr>
<tr>
<td>❑ Cancel Provision</td>
<td>Cancel a previously scheduled provisioning operation. To select devices, you must click the checkbox for the device. You can cancel provisioning for multiple devices at one time. You cannot cancel device provisioning once it has started.</td>
</tr>
<tr>
<td>❑ Clear Status</td>
<td>Change the status column for a device to the Clear state</td>
</tr>
</tbody>
</table>

For information about these device commands, see “Device Provisioning Operations” on page 83.
Automatic Softupdate View

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

Device List in the Automatic Softupdate View

By default the **Device List** in the **Automatic Softupdate View** displays all devices eligible for automatic softupdate.

The device list in the **Automatic Softupdate View** has the following information.

**Table 7-6 Fields of the Device List in the Automatic Softupdate View**

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

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

Scheduled Softupdate View

Use the Scheduled Softupdate View, available from the Device menu, to:

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

Device List in the Scheduled Softupdate View

By default the Device List in the Scheduled Softupdate View displays all devices eligible for scheduled softupdate.

The device list in the Scheduled Softupdate View has the following information.

Table 7-7  Fields of the Device List in the Scheduled Softupdate View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Filter choices for this view include:</td>
</tr>
<tr>
<td></td>
<td>• Type - Filters the device list by device type</td>
</tr>
<tr>
<td></td>
<td>• Name - Searches the device list by system name</td>
</tr>
<tr>
<td></td>
<td>• IP Address - Searches the device list by device IP address</td>
</tr>
<tr>
<td></td>
<td>• ISDN Video Number - Searches the device list by device ISDN video number</td>
</tr>
<tr>
<td></td>
<td>• Alias - Searches the device list by device alias</td>
</tr>
<tr>
<td></td>
<td>• Site - Searches the device list by device site location</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the device's last scheduled softupdate. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Clear</td>
</tr>
<tr>
<td>Name</td>
<td>The system name of the device</td>
</tr>
</tbody>
</table>
**Table 7-7  Fields of the Device List in the Scheduled Softupdate View**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of device. Scheduled softupdate is only available for these device types:</td>
</tr>
<tr>
<td></td>
<td>• HDX-Series—Polycom HDX systems operating in standard (non-dynamic) management mode</td>
</tr>
<tr>
<td></td>
<td>• V-Series or VSX-Series</td>
</tr>
<tr>
<td></td>
<td>• ViewStation FX and EX</td>
</tr>
<tr>
<td></td>
<td>• ViewStation</td>
</tr>
<tr>
<td></td>
<td>• Tandberg MXP Series endpoints</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address assigned to the device</td>
</tr>
<tr>
<td>Current Version</td>
<td>The version of software installed during the last successful softupdate procedure</td>
</tr>
<tr>
<td>Scheduled</td>
<td>When the device is scheduled for softupdate, this field shows the date and time for the scheduled softupdate process</td>
</tr>
</tbody>
</table>

**Scheduled Softupdate View Commands**

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

**Table 7-8  Device Commands - Scheduled Softupdate View**

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Device</td>
<td>Manually add a device to the Polycom CMA system</td>
</tr>
<tr>
<td>✔️ Software Update</td>
<td>Schedule softupdate for the selected device(s). To select devices, you must select the checkbox for the device. You can schedule softupdates for multiple devices at one time.</td>
</tr>
<tr>
<td>✔️ Cancel Update</td>
<td>Cancel a previously scheduled softupdate operation. To select devices, you must select the checkbox for the device. You can cancel softupdates for multiple devices at one time. You cannot cancel a softupdate once it has started.</td>
</tr>
<tr>
<td>✔️ Clear Status</td>
<td>Change the status column for a device to the <strong>Clear</strong> state</td>
</tr>
</tbody>
</table>

For information about these device commands, see “Device Softupdate Operations” on page 91.
Device Types

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

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full support in dynamic management mode—Gatekeeper registration, GAB registration, automatic provisioning, automatic softupdate, and presence</strong></td>
<td></td>
</tr>
<tr>
<td>Polycom CMA Desktop</td>
<td>Version 1.0 or greater</td>
</tr>
<tr>
<td>HDX-Series</td>
<td>Polycom HDX systems version 2.5 or greater</td>
</tr>
<tr>
<td><strong>Full support in standard management mode—Gatekeeper registration, GAB registration, scheduled provisioning, and scheduled softupdate</strong></td>
<td></td>
</tr>
<tr>
<td>HDX-Series</td>
<td>Polycom HDX systems version 1.0 or greater operating in standard (non-dynamic) management mode</td>
</tr>
<tr>
<td>ViewStation</td>
<td>None</td>
</tr>
<tr>
<td>ViewStation FX and EX</td>
<td>None</td>
</tr>
<tr>
<td>V-Series or VSX-Series</td>
<td>None</td>
</tr>
<tr>
<td>Tandberg MXP Series endpoints</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Limited support in standard management mode—Gatekeeper registration and GAB registration only</strong></td>
<td></td>
</tr>
<tr>
<td>iPower</td>
<td>iPower support is being phased out</td>
</tr>
<tr>
<td>PVX</td>
<td>None</td>
</tr>
<tr>
<td>Tandberg MXP Series endpoints</td>
<td>The Polycom CMA system supports gatekeeper and GAB registration on Tandberg 6000, Edge95, 1700, 1500 endpoints</td>
</tr>
<tr>
<td><strong>Third party support—Gatekeeper registration only</strong></td>
<td></td>
</tr>
<tr>
<td>Sony PCS Version 03.00</td>
<td>None</td>
</tr>
<tr>
<td>Aethra Maia Starr Version 5.1.35</td>
<td>None</td>
</tr>
<tr>
<td>VCON (Galaxy and Vigo) Version 0202.M05.D28.H12</td>
<td>None</td>
</tr>
<tr>
<td>VTEL, all versions</td>
<td>None</td>
</tr>
</tbody>
</table>
A Polycom CMA system also supports these Polycom MCUs:

- MGC
- RMX 2000 and RMX 1000

**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 RMX 1000 MCUs.

A Polycom CMA system may also list these device types:

- **Other** - A Polycom CMA system cannot control endpoints with a device type of Other and cannot direct these devices to initiate point-to-point calls. A scheduled point-to-point call between two video endpoint systems with a device type of Other requires the use of an MCU.
- **GW/MCU** - H.323 cards and IP blades in Polycom MCUs are assigned the device type of GW/MCU during registration.

**Note**

In the Device > Admin/Monitor View, a Polycom CMA system displays MCUs as two separate Device Types, the MCU type and a GW/MCU device. The GW/MCU designation represents the network interface.

If automatic registration is allowed, individual H.323 cards/IP blades in the MGC automatically register separately and appear as GW/MCU devices. If automatic registration is not allowed, you must add a device record for each H.323 card and IP blade.

### Device Configuration/Provisioning

The Polycom CMA system device provisioning, which requires 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.
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 system devices deployed in dynamic management mode
- Polycom CMA Desktop systems

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

How Automatic Device Provisioning Works

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

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 tables shows the fields you can define when adding a new automatic provisioning profile.

Note
Polycom CMA Desktop provisioning occurs on a session by session basis.
Table 7-9  Automatic Device Provisioning Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audio Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Mute Auto Answer Calls</td>
<td>Specifies whether or not to automatically mute incoming calls</td>
</tr>
<tr>
<td><strong>Call Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Preferred Dialing Method</td>
<td>Specifies the preferred method for dialing various call types.</td>
</tr>
<tr>
<td></td>
<td>• If set to <strong>Auto</strong>, calls use the configured dialing order.</td>
</tr>
<tr>
<td></td>
<td>• If set to <strong>Manual</strong>, the endpoint systems will prompt the user to select the call type from a list when placing a call.</td>
</tr>
<tr>
<td><strong>Home Screen Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Display Contact List as Home Screen</td>
<td>Specifies whether or not to display the contact list as the entry screen</td>
</tr>
<tr>
<td>Display H.323 Extension</td>
<td>Lets users placing a gateway call enter the H.323 extension separately from the gateway ID.</td>
</tr>
<tr>
<td></td>
<td>If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format: gateway ID + ## + extension</td>
</tr>
<tr>
<td>Enable Availability Control</td>
<td>When enabled, lets users set their availability in the endpoint system's local user interface.</td>
</tr>
<tr>
<td><strong>H.323 Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum Speed for Receiving Calls (kbps)</td>
<td>Allows you to restrict the bandwidth used when receiving calls.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Preferred Speed for Placing Calls (kbps)</td>
<td>Determines the speeds that will be used for calls from this endpoint system when:</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Call Quality</strong> selection is either unavailable or set to <strong>Auto</strong> on the <strong>Place a Call</strong> screen</td>
</tr>
<tr>
<td></td>
<td>• The call is placed from the directory</td>
</tr>
<tr>
<td></td>
<td>If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.</td>
</tr>
</tbody>
</table>
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-Bandwidth 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 management mode, administrators with System Setup permissions 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
- ViewStation FX & EX
- V-Series (V- and VSX-systems)
- Tandberg MXP series endpoints
- HDX-Series--Polycom HDX system devices deployed in standard 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

Some notes about scheduled provisioning of devices:

- Until the Polycom CMA system successfully provisions a device scheduled for provisioning, provisioning remains in the Pending state and the system attempts to provision the device until it succeeds or until the provisioning is cancelled.
Device Management Overview

- If a device scheduled for provisioning is **In a Call**, the system waits until the call ends before provisioning the device. The system checks the endpoint at 15 minute intervals.
- If a device scheduled for provisioning is **Offline**, the system attempts to connect to the device at 60 minute intervals until the device is **Online**.
- Provisioning may reboot the device.
- You can schedule provisioning for as many devices as desired at one time, but the system may limit the number of active provisioning processes.

### Device 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 checks with the Polycom CMA system to determine if it should download a newer softupdate package. If a softupdate is necessary, the package is sent in XML format over a secure HTTPS connection.

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 Series and VSX Series
- Tandberg MXP series
- HDX-Series--Polycom HDX system devices operating in standard management mode

Some notes about scheduled softupdates:

- Until the Polycom CMA system successfully updates a device scheduled for updating, the update remains in the **Pending** or **In Progress** state and the Polycom CMA system attempts to update the device until it succeeds or until the update is cancelled.
• If a device scheduled for update is In a Call, the Polycom CMA system waits until the call ends before updating the device. The system checks the endpoint at 15 minute intervals.

• If a device scheduled for update is Offline, the Polycom CMA system attempts to connect to the device every hour until the device is Online.

• A software update may reboot the device.

Device Passwords

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

• Provision a device through a Polycom CMA system
• Use the Softupdate feature
• Monitor the device from the Device > Admin/Monitor View

For security reasons, you must set a password at the endpoint first and then in the Polycom CMA system. (The password field is ASCII only; for more information, see “Field Input Requirements” on page 6.)

After you have entered the matching password in the Polycom CMA system, you can update the password for certain devices through provisioning. 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 devices, passwords may be required to access the device management software.

For information about restrictions in changing passwords for a specific device, see the documentation for the device.
Device Management Operations

This chapter describes how to perform the Polycom® Converged Management Application™ (CMA™) system device management tasks.

- View Device Details
- Add an Endpoint or Find an Endpoint on the Network
- Add an MCU Manually
- Edit a Device
- Delete a Device
- View a Device’s Video Feed
- Clear a Device Help Request
- Send a Message to a Device

View Device Details

To view detailed information about a managed device

1. Go to Device > Admin/Monitor View.
2. As needed, use the Filter to customize the device list.
3. Select the device of interest and click View Device Details.

The Device Details dialog box for the selected device appears. For more information, see “Device Details” on page 103.
Add an Endpoint or Find an Endpoint on the Network

Generally, the devices the Polycom CMA system manages are either endpoints or MCUs. This section describes how to manually add endpoints and how to find endpoints on the same network as the Polycom CMA system.

If the Polycom CMA gatekeeper registration policy allows devices to register automatically (i.e., a gatekeeper setting of Allow Registration of All Endpoints or Allow Registration of Endpoints in a Defined Site), those registered devices (Polycom devices or third-party devices) are automatically added to the device list. If a device is not registered with the gatekeeper and it has a web-based interface, you can enter the device information manually and manage the device directly from the Admin/Monitor View.

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 video endpoint systems and MCUs to the CMA system. However, devices registered to the Global Address Book are automatically added to the Polycom CMA system.

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

For most endpoints, you enter basic information. The Polycom CMA system then contacts the endpoint and retrieves device details, which includes the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find Device on Network</td>
<td></td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of device. For valid device types, see &quot;Device Types&quot; on page 61.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the device</td>
</tr>
<tr>
<td>System Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td></td>
<td>• Device names must be unique.</td>
</tr>
<tr>
<td></td>
<td>• The name must be in ASCII only and may have an unlimited number of characters. Spaces,</td>
</tr>
<tr>
<td></td>
<td>dashes, and underscores are valid.</td>
</tr>
<tr>
<td></td>
<td>• When retrieved from a video endpoint system, the name is taken from the H.323 ID if the</td>
</tr>
<tr>
<td></td>
<td>device registered with the gatekeeper and it is a third-party system. In other cases, it is</td>
</tr>
<tr>
<td></td>
<td>the system name, which might be different than the H.323 ID.</td>
</tr>
<tr>
<td></td>
<td>• For an MGC or RMX 2000 device, you must type in a device name.</td>
</tr>
<tr>
<td>Admin ID</td>
<td>The administrator ID for the device</td>
</tr>
<tr>
<td>Password</td>
<td>The administrator password for the device</td>
</tr>
</tbody>
</table>
### Table 8-1 Fields of the Add Device

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>•</td>
<td>Device names must be unique.</td>
</tr>
<tr>
<td>•</td>
<td>The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.</td>
</tr>
<tr>
<td>•</td>
<td>When retrieved from a video endpoint system, the name is taken from the H.323 ID if the device 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.</td>
</tr>
<tr>
<td>•</td>
<td>For an MGC or RMX 2000 device, you must type in a device name.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-form text field (Extended ASCII only) in which information about the device can be added</td>
</tr>
<tr>
<td>Site</td>
<td>The network site for the device. By default, devices are added to the <strong>Primary Site</strong>.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td><strong>HTTP URL</strong></td>
<td>(Endpoints only) The management URL for the device, if available (ASCII only). This URL allows operators to manage the device from the Device &gt; Admin/Monitor View &gt; Manage Device screen.</td>
</tr>
<tr>
<td></td>
<td>All Polycom endpoints provide device management through a browser. For these devices, this field is completed when the device registers with the CMA system.</td>
</tr>
<tr>
<td></td>
<td>For third-party endpoints and devices that do not register using an IP address, you must enter the URL.</td>
</tr>
<tr>
<td><strong>HTTP Port</strong></td>
<td>(Endpoints only) The HTTP port number for the device. The device provides the port number if it registered successfully and is managed.</td>
</tr>
<tr>
<td><strong>Addresses</strong></td>
<td></td>
</tr>
<tr>
<td>DNS Name</td>
<td>Name for the device as assigned at the Domain Name Service.</td>
</tr>
</tbody>
</table>
### Table 8-1 Fields of the Add Device

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aliases</strong></td>
<td>The alias to connect to the device. The CMA system converts the aliases to the IP address associated with the device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alias Type</strong>. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Alias Value</strong>. Value for the alias type shown.</td>
</tr>
<tr>
<td></td>
<td>• The value for the H.323 ID is the device name if the device registered with the gatekeeper and it is a third-party system. In other cases, the device name is the system name, which might be different then the H323 ID.</td>
</tr>
<tr>
<td></td>
<td>• The value of the E.164 alias is the extension dialed to reach this endpoint.</td>
</tr>
<tr>
<td></td>
<td>• To add another alias, select the type, enter the value (ASCII only), and click <strong>Add Alias</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To remove an alias, select it and click <strong>Delete Selected Row</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The following <strong>Alias Values</strong> are ASCII only: H323 ID, URL, Transport Address, and Unknown.</td>
</tr>
<tr>
<td><strong>ISDN Video Number</strong></td>
<td>For ISDN devices only, the country code + city/area code + phone number for the device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Capabilities</strong></td>
<td>The communications protocols that the device can support. Possible values include:</td>
</tr>
<tr>
<td><strong>Supported Protocols</strong></td>
<td>• <strong>IP (H.323)</strong> - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ISDN (H.320)</strong> - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.</td>
</tr>
<tr>
<td></td>
<td>For devices with the type <strong>Unknown</strong>, select <strong>H.323</strong>.</td>
</tr>
<tr>
<td></td>
<td>The device automatically provides the protocols if it registered successfully or is managed.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>• If an endpoint is configured as a gateway (ISDN), only the <strong>H.323</strong> checkbox is selected. If the endpoint supports true ISDN, the <strong>H.323 and ISDN</strong> checkboxes are selected.</td>
</tr>
<tr>
<td></td>
<td>• RMX 2000 devices support only the <strong>H.323</strong> protocol.</td>
</tr>
<tr>
<td><strong>Capabilities Enabled</strong></td>
<td>Capabilities to enable on this device. Options are:</td>
</tr>
<tr>
<td><strong>MCU</strong></td>
<td>• The device can act as a control unit for multipoint conferences</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>• The device can act as a gateway for call management</td>
</tr>
<tr>
<td></td>
<td>The MCU provides the capability if it registered successfully or is managed.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Currently, RMX 2000 devices cannot be Gateway devices.</td>
</tr>
</tbody>
</table>
To add an endpoint to a Polycom CMA system or find an endpoint on the network

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

### Table 8-1  Fields of the Add Device

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available to Schedule</td>
<td>Select this option to make the device available when users are scheduling conferences</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The Available to schedule field is empty and disabled for MGC and RMX 2000 devices.</td>
</tr>
<tr>
<td>Monitoring Level</td>
<td>The monitoring level for the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Standard. This device is monitored.</td>
</tr>
<tr>
<td></td>
<td>• VIP. This device is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.</td>
</tr>
</tbody>
</table>

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

### Note

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

- V-Series, VSX-Series, and Viewstation devices allow the Polycom CMA system to detect the device type and complete the registration. The device appears in the Device List with an alert indicating Incorrect Password.
- Polycom HDX systems and ViewStation FX systems won’t allow the Polycom CMA system to detect the device type and complete the registration. You can manually add the device, but the Polycom CMA system cannot communicate with it until you’ve entered a valid Admin ID or Password for the device. 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 Table 8-1.) At a minimum, assign the device a System Name.

Pay particular attention to the Capabilities options, because the settings on it determine how the device is used throughout the Polycom CMA system. For example, you can select it as a VIP device 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 information about field input requirements, see “Field Input Requirements” on page 6.

8 Click Add.

The device appears in the Device List. By default, the system:

- Adds the device to the applicable site
- Sets the HTTP Port to 80
- Adds an Alias for the device
- Makes the device 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 a device, you can associate it with a user. See “Assign Users Roles and Devices” on page 128.

### Add an MCU Manually

Generally, the devices the Polycom CMA system manages are either endpoints or MCUs. This section describes how to add an MCU to a Polycom CMA system.

Note
Back-end communication with the RMX 2000 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.
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**—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.

### Notes
- RMX 2000 devices may only have H.323 service.
- 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 H.323 service on the MCU, when the Polycom CMA system tries to schedule a video conference that requires this service, it tries to locate another MCU with this service. If another MCU with this service is not available, the conference may not be scheduled.

MCU device details include these fields.

**Table 8-2**  **Fields in the MCU H.320 Service Dialog Box (MGC Only)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Name of the H.320 ISDN service</td>
</tr>
<tr>
<td>Channels</td>
<td>Number of 64K channels dedicated to the MCU</td>
</tr>
<tr>
<td>Number Range</td>
<td>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).</td>
</tr>
<tr>
<td>LCR Table</td>
<td>The least-cost routing table for calls made through this gateway</td>
</tr>
<tr>
<td>Local Prefix</td>
<td>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.</td>
</tr>
</tbody>
</table>
To add or register an MCU to a Polycom CMA system

1  Go to Device > Admin/Monitor View and click Add Device.
2  In the Add New Device dialog box, select the Device Type of interest. For valid device types, see “Device Types” on page 61.
3  Enter the IP Address of the device.
4  If necessary, enter the Admin ID and Password for the device.
5  Click Find Device.
   — If the Polycom CMA system can find the device on the network, the Add New Device dialog box is populated with information retrieved from the device. Review any information retrieved from the device.
   — If the Polycom CMA system cannot find the device, a Device Not Found dialog box appears. Click OK.
6  Complete the Identification, Addresses, Capabilities, MCU Services and MCU Resources sections of the Add New Device dialog box. (For more information, see Table 8-1.) Pay particular attention to the Capabilities options, because the settings on it determine how the device is used throughout the Polycom CMA system. For example, you can designate a Polycom MGC as a Gateway device.

Note that many fields in this dialog box are ASCII only. For information about field input requirements, see “Field Input Requirements” on page 6.

7  Click Add.

The device appears in the Device List. By default, the system:
   — Adds the device to the Primary Site
   — Sets the HTTP Port to 80
   — Adds an Alias Type for the devices
Edit a Device

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

To edit a device in the Polycom CMA system

1. Go to Device > Admin/Monitor View
2. As needed, use the Filter to customize the device list.
3. Select the device of interest and click Edit Device.
4. As required, edit the Addresses, Capabilities, and if applicable MCU Services and MCU Resources, sections of the Edit Device dialog box. (For more information, see Table 8-1.)

   Note that many fields in this dialog box are ASCII only. For information about field input requirements, see “Field Input Requirements” on page 6.
5. Click Update.

Note

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

**To delete a device from the Polycom CMA system**

1. Go to Device > Admin/Monitor View
2. As needed, use the Filter to customize the device list.
3. Select the device of interest and click Delete Device.
4. Click Yes to confirm the deletion.
   The Device List is updated.

**Note**
If your gatekeeper registration policy allows devices to register automatically with the Polycom CMA system (i.e., a gatekeeper setting of Allow Registration of All Endpoints or Allow Restoration of Endpoints in a Defined Site), a device that you delete may reappear in the Device List.

View a Device’s Video Feed

**Note**
This procedure is available on the following device types:
- Polycom HDX system
- Tandberg
- V-Series and VSX-Series
- ViewStation

**To view the video feed for a device (near site or far site)**

1. Go to Device > Admin/Monitor View
2. As needed, use the Filter to customize the device list.
3. Select the device of interest and click View Device Details.
   The Device Details dialog box appears. For information about the fields in this dialog box, see Table 8-1.
4. Click Call Info to expand the Call Info tree and select Video Feed.
   The Device Video section shows the video feed from the near and far site.
5. To view updated feed information, refresh your display.
Clear a Device Help Request

To clear a device help request from the Polycom CMA system
1. Go to Device > Admin/Monitor View
2. As needed, use the Filter to customize the device list.
3. Select the device of interest and click Clear Help.
   The Confirm Device Help Clear dialog box appears.
4. To send a message to the device as well as clear the help request, click the Also send message to device checkbox.
5. Click Yes.
6. If you selected the Also send message to device checkbox, enter the text message to send the device in the Send Message to Device 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 Device List is updated and alerts for the device are cleared.

Note
If the reason for the original alert still exists on the device, the alert will likely reappear in the Device List.

Send a Message to a Device

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

To send a message to a device from the Polycom CMA system
1. Go to Device > Admin/Monitor View
2. As needed, use the Filter to customize the device list.
3. Select the device of interest.
   If the device can receive text messages, a Send Message option appears in the Command menu.
4. Click Send Message.
   The Confirm Device Alert dialog box appears.
5 In the **Send Message to Device** 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 device.
Device Provisioning Operations

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

For automatic device provisioning, it includes these topics:

• 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 device provisioning, it includes these topics:

• View the Scheduled Device 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 a Device for Provisioning
• Check the Status of a Scheduled Device Provisioning
• Clear the Status of Scheduled Device Provisioning
• Cancel a Scheduled Device Provisioning
**Automatic Provisioning Operations**

**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 device 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 **System Management > Profiles/Policies > Automatic Provisioning Profiles**.
2. From the **Automatic Provisioning Profiles** screen, click **Add Profile**.
3. In the **Add Profile** dialog box, enter a name for the profile and click **Next**.
4. Complete the **Audio Settings**, **Call Settings**, **Home Screen Settings**, **H.323 Settings**, and (if applicable) **CMA Desktop Settings** sections of the **Provisioning Fields** dialog box. The sections differ depending on the device 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 System Management > Profiles/Policies > Automatic Provisioning Profiles.
2 From the Automatic Provisioning Profiles screen, 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 device type selected. For more information on these fields, see the product documentation for the selected endpoint.
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 System Management > Profiles/Policies > Automatic Provisioning Profiles.
2 From the Automatic Provisioning Profiles screen, select the profile of interest and 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 System Management > Profiles/Policies > Automatic Provisioning Profiles.
2 From the Automatic Provisioning Profiles screen, 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 Automatic Provisioning Profiles list.
4 As needed, edit the cloned profile.
Delete an Automatic Provisioning Profile

To delete an automatic provisioning profile

2. From the Automatic Provisioning Profiles screen, 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.

Scheduled Provisioning Operations

View the Scheduled Device Provisioning List and Details

To view information about device provisioning

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

Add a Scheduled Provisioning Profile

To add a scheduled provisioning profile

2. From the Scheduled Provisioning Profiles screen, click Add Profile.
3. In the Add Profile dialog box, select the Device Type for the provisioning profile, enter a name for the profile, and click Next.

   The Provisioning Fields dialog box appears with default content based on the Device Type you selected.

4. Complete the sections of the Provisioning Fields dialog box. The sections differ depending on the device type selected. For more information on these fields, see the product documentation for the selected endpoint.
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 System Management > Profiles/Policies > Scheduled Provisioning Profiles.
2 From 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 device type selected. For more information on these fields, see the product documentation for the selected endpoint.
4 Click OK.
   The provisioning profile is updated.

Clone a Scheduled Provisioning Profile

To clone a scheduled provisioning profile

1 Go to System Management > Profiles/Policies > Scheduled Provisioning Profiles.
2 From the Scheduled Provisioning Profiles screen, 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.

Delete a Scheduled Provisioning Profile

To delete a scheduled provisioning profile

1 Go to System Management > Profiles/Policies > Provision Device Profiles.
2 From the Scheduled Provisioning Profiles screen, 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 a Device for Provisioning**

**To schedule a device for provisioning**

1 Go to Device > Scheduled Provisioning View.

2 As needed, use the Filter to customize the device list.

3 Select the device of interest. To select all devices of that type, click the checkbox in the column header.

4 Click Provision.

5 In the Schedule Device 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 Device Date/Time as these may differ.

9 Click Schedule.

The Scheduled Provisioning View reappears.

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

   For each device 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 Device Provisioning**

**To check the status of device provisioning**

1 Go to Device > Scheduled Provisioning View.

2 As needed, use the Filter to customize the device list.

3 Select the device 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 Device Provisioning List and Details” on page 86.
Clear the Status of Scheduled Device Provisioning

To clear the status of device provisioning

1. Go to Device > Scheduled Provisioning View.
2. As needed, use the Filter to customize the device list.
3. Select the device of interest. To select all devices in the list, click the checkbox in the column header.
4. Click Clear Status.

   The device provisioning status returns to Clear.

Cancel a Scheduled Device Provisioning

You can only cancel provisioning of a Pending profile. You cannot cancel the provisioning of a device while it is In Progress.

To cancel a pending scheduled device provisioning

1. Go to Device > Scheduled Provisioning View.
2. As needed, use the Filter to customize the device list.
3. Select the device of interest. To select all devices in the list, click the checkbox in the column header.
4. Click Cancel Provision.

   The provisioning operation is cancelled and the device provisioning status returns to Clear.
This chapter section describes how to use Polycom® Converged Management Application™ (CMA™) system to update the software on Polycom devices when a new software package is available.

For automatic device softupdate, it includes these topics:

- View Automatic Softupdate Information
- View Automatic Softupdate Profiles
- Implement Automatic Softupdates for Devices

For scheduled device softupdate, it includes these topics:

- View Scheduled Softupdate Information
- View List of Softupdate Profiles
- Implement Scheduled Softupdates for Devices

### Automatic Softupdate Operations

#### View Automatic Softupdate Information

To view information for devices that are eligible for automatic softupdates

1. Go to Device > Automatic Softupdate View.

   The **Automatic Softupdate View** appears.

2. As needed, use the **Filter** to customize the device list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.

3. Select the device of interest.

4. In the **Device Details** section, expand the **Softupdate Details** tab. For more information, see “Softupdate Details” on page 109.
View Automatic Softupdate Profiles

To view the list of automatic softupdate profiles

1. Go to System Management > Profiles > Automatic Software Updates.

   The Automatic Software Updates screen appears and the HDX-Series automatic softupdate profiles are displayed.

Table 10-1 Fields of the Automatic Software Updates screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version to use</td>
<td>Displays the default automatic softupdate profile to be used for the device type and model</td>
</tr>
<tr>
<td>Allow this version or newer</td>
<td>When checked, indicates that whenever a newer automatic softupdate profile for the device type and model is added, that profile should be used as the default automatic softupdate profile</td>
</tr>
<tr>
<td>Device Type</td>
<td>The type of device. For valid device types, see “Device Types” on page 61.</td>
</tr>
<tr>
<td>Device Model</td>
<td>The model of device</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the software package associated with the automatic provisioning profile</td>
</tr>
<tr>
<td>Description</td>
<td>The meaningful name given to the automatic softupdate profile when it was created</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The date and time when the automatic softupdate profile was created</td>
</tr>
</tbody>
</table>

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

Implement Automatic Softupdates for Devices

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

1. “List the Serial Numbers for the Devices to be Updated” on page 93.
2. “Download the Required Software Package” on page 94.
3. “Request Update Activation Keys” on page 94.
4. “Upload the Software Package and Create a Softupdate Profile” on page 95. For more information on softupdate profiles, see “View Automatic Softupdate Information” on page 91.
List the Serial Numbers for the Devices to be Updated

To list the serial numbers for the devices to be updated

1. Go to System Management > Profiles > Automatic Software Updates.

2. Click Get Serial Number.

   The Device Serial Number List appears listing the devices eligible for automatic softupdate.

3. Select the specific device(s) to be updated. To select all devices in the list, click the checkbox in the column header.

4. Click Get Serial Numbers.

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

5. When updating a single device:
   a. Record the serial number: ________________________________
   b. Click Close.

      The Automatic Software Updates list reappears.

   c. Go to “Download the Required Software Package” on page 94.

6. When updating multiple devices:
   a. Copy and paste the serial numbers from the Device 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 Device Serial Number List and click Close.

      The Automatic Software Updates list reappears.

   c. Repeat steps 2 through 6 for 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.

   e. Go to “Download the Required Software Package” on page 94.
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. If the software package is in a compressed format, extract the software package.
6. Repeat steps 3 through 5 for each device type and model to be updated.

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

2. Log in or Register for An Account.
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 6 on page 93):
   a In the Multiple Upgrade KeyCode section, click Add Attachment.
   b Browse to the location of the .txt file you created in step 6 on page 93 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

After you receive notification about a new software package for a Polycom device, 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 System Management > Profiles > Automatic Software Updates.
2 Click Upload Software Update.
3 In the Upload Software Update dialog box, verify the device type and model.
4 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 94).

**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.
   An automatic softupdate profile for the device type and model type appears in the Automatic Software Update list.
   If you receive a message that indicates “This version is the first for its device type, so it will be assumed to be the policy for this device type,” the softupdate profile also appears in the Version to use field.
7 To ensure that newer softupdate profiles for each device type and model, select the **Use a newer version if available** option and click **Update**.

**Scheduled Softupdate Operations**

**View Scheduled Softupdate Information**

To view information about softupdates that are scheduled or for devices that are eligible for scheduled softupdates

1 Go to **Device > Scheduled Softupdate View**.

2 As needed, use the **Filter** to customize the device list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, and **Site**.

3 Select the device of interest.

4 In the **Device Details** section, expand the **Softupdate Details** tab. For more information, see “**Softupdate Details**” on page 109.

**View List of Softupdate Profiles**

To view the list of scheduled softupdate profiles

>> Go to **System Management > Profiles > Scheduled Software Updates**.
The **Scheduled Software Updates** screen appears.

**Table 10-2 Fields of the Scheduled Software Updates screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>The type of device. For valid device types, see “<strong>Device Types</strong>” on page 61.</td>
</tr>
<tr>
<td>Device Model</td>
<td>The model of device</td>
</tr>
<tr>
<td>Description</td>
<td>The meaningful name given to the automatic softupdate profile when it was created</td>
</tr>
<tr>
<td>Uploaded</td>
<td>The date and time when the scheduled softupdate profile was created</td>
</tr>
</tbody>
</table>
Implement Scheduled Softupdates for Devices

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

1. “List the Serial Numbers for the Devices to be Updated” on page 97.
2. “Download the Required Software Package” on page 98.
3. “Request Update Activation Keys” on page 98.
4. “Upload the Software Package and Create a Softupdate Profile” on page 99. For more information on softupdate profiles, see “View Automatic Softupdate Information” on page 91.
5. “Schedule the Softupdate for Devices” on page 100.

List the Serial Numbers for the Devices to be Updated

To list the serial numbers for the devices to be updated

1. Go to System Management > Profiles > Scheduled Software Updates.
2. Select the appropriate Device Type and Device Model combination for the device(s) to update. To select all devices in the list, click the checkbox in the column header.
3. Click Get Serial Number.
   The Device Serial Number List appears listing the devices of the selected type and model that are eligible for scheduled softupdates.
4. Select the device of interest. 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 screen.
6. When updating a single device:
   a. Record the serial number:_____________________________________
   b. Click Close.
   The Scheduled Software Updates list reappears.
7. When updating multiple devices:
   a. Copy and paste the serial numbers from the Device 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.

820/1UU/111DA/U
82070407E010CD
820418048078B2
82040903E00FB0

b Return to the Device Serial Number List and click Close. The Scheduled Software Updates list reappears.

c Repeat steps 2 through 7 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 If the software package is in a compressed format, extract the software package.

6 Repeat steps 3 through 5 for each device type and model to be updated.

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:
Device Softupdate Operations

- **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 6 on page 93):

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

- **b** Browse to the location of the .txt file you created in step 6 on page 93 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 **System Management > Profiles > Scheduled Software Updates**.

2 On the **Software Update Profiles** list, click the checkbox to select the appropriate **Device Type** and **Device Model** combination for the device(s) to be updated. To select all devices in the list, click the checkbox in the column header..

3 In the **Upload Software Update** dialog box, verify the device 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 94).

**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](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 device type and model type is created.

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

Schedule the Softupdate for Devices

To schedule one or more devices for softupdate

1 Go to Device > Scheduled Softupdate View.

2 As needed, use the Filter to customize the device list.

3 Select the device(s) of interest and click Software Update. To select all devices in the list, click the checkbox in the column header.

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 Device Date/Time as these may differ.

5 Select from these options.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove address book entries</td>
<td>Select this checkbox to have all local address book entries removed after the update.</td>
</tr>
<tr>
<td>Remove System Files</td>
<td>Select this checkbox to have all endpoint settings removed after the update. You must then reconfigure the device.</td>
</tr>
<tr>
<td>Allow endpoint to be a DHCP server</td>
<td>Select this checkbox to allow the endpoint to be a DHCP server. Applies to V-Series, VSX-Series, and ViewStation devices only. For more information, see the endpoint’s user guide.</td>
</tr>
<tr>
<td>Passive Mode</td>
<td>Select this checkbox to perform a softupdate in passive FTP mode. Applies to V-Series, VSX-Series, and ViewStation devices only. For more information, see the endpoint’s user guide.</td>
</tr>
</tbody>
</table>
6 Click Schedule.

For each device 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 a device. You cannot explicitly cancel automatic softupdates for a device. You must do that at the endpoint.

**To cancel pending software updates**

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

The software update operation is cancelled. The device’s status returns to Clear.

---

**Note**

You may apply a single softupdate request to multiple device models. If the request includes one or more scheduling options that are not valid for a selected device model, the system applies only the options that are valid.
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
- Device Status Information
- Call Information
- Device Alerts Information
- Provisioning Details
- Softupdate Details

Device Summary Information

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device. For valid device types, see &quot;Device Types&quot; on page 61.</td>
</tr>
<tr>
<td>Owner (Endpoints only)</td>
<td>(Endpoints only) The user associated with the device</td>
</tr>
<tr>
<td>IP Address</td>
<td>The assigned IP address of the device</td>
</tr>
<tr>
<td>ISDN Video Number</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 11-1  Device Summary Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>The network site for the device. By default, devices are added to the <strong>Primary Site</strong>.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number (ASCII only) of the device. The device provides the serial number if it registered successfully or is managed.</td>
</tr>
</tbody>
</table>
| 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. |
Device Status Information

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

### Table 11-2  Device Status Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  |
### Table 11-2  Device Status Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GK Registration Timeout</td>
<td>The gatekeeper registration expiration date and time for the device in a default format of mm-dd-yyyy hh:mm:ss AM</td>
</tr>
<tr>
<td>Last GK Registration</td>
<td>The date and time of the device’s last gatekeeper registration in a default format of mm-dd-yyyy hh:mm:ss AM</td>
</tr>
<tr>
<td>Device Local Time</td>
<td>The local time as set within the device in a default format of hh:mm:ss AM</td>
</tr>
<tr>
<td>ISDN Line Status Type</td>
<td>The status of the ISDN line. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Operational • Non-operations</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and Tandberg.</td>
</tr>
<tr>
<td>ISDN Assignment Type</td>
<td>How the ISDN type was assigned to the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Administrator, when the ISDN type was assigned manually by an administrator</td>
</tr>
<tr>
<td></td>
<td>• Endpoint, when the ISDN type was natively assigned in the endpoint</td>
</tr>
<tr>
<td></td>
<td>• Auto-Assigned, when the ISDN type was automatically assigned by the CMA system based on the site configuration</td>
</tr>
<tr>
<td></td>
<td>• From Network, when the ISDN type was derived from the gateway and extension</td>
</tr>
<tr>
<td></td>
<td>• Undefined, when the CMA system cannot identify the source for the ISDN type assignment</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and Tandberg.</td>
</tr>
<tr>
<td>Endpoint ISDN Type</td>
<td>The ISDN network interface type installed in the device. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• ISDN_QUAD_BRI • ISDN_PRI_T1 • ISDN_BRI • ISDN_UNKNOWN</td>
</tr>
<tr>
<td></td>
<td>This field is blank for the following device types: PVX, MGC, RMX, GW/MCU, Other, and Tandberg.</td>
</tr>
</tbody>
</table>
The **Call Info** in the **Device Details** section includes the following fields.

### Table 11-3 Call Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Type</td>
<td>The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and SIP</td>
</tr>
<tr>
<td>Video Protocol</td>
<td>The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• H.261</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• H.263</td>
</tr>
<tr>
<td></td>
<td>H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions.</td>
</tr>
<tr>
<td></td>
<td>• H.264</td>
</tr>
<tr>
<td>Video Format</td>
<td>The video format, both transmission (Tx) and reception (Rx), the device is using.</td>
</tr>
<tr>
<td>Audio Protocol</td>
<td>The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• G.711</td>
</tr>
<tr>
<td></td>
<td>• G.722</td>
</tr>
<tr>
<td></td>
<td>• G.728</td>
</tr>
<tr>
<td>Far Site Name</td>
<td>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 '</td>
</tr>
<tr>
<td>Far Site Number</td>
<td>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.</td>
</tr>
<tr>
<td>Cause Code</td>
<td>Standard H.323 cause code that reflects normal call termination or the nature of an internal failure, e.g., '16' or '211'.</td>
</tr>
<tr>
<td>Encryption</td>
<td>The status of encryption for the call. Possible values include: Off, Disabled, AES, and DH-1024</td>
</tr>
</tbody>
</table>
Device Alerts Information

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

**Table 11-4  Device Alerts Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Device error message text, e.g., GK Registration error</td>
</tr>
<tr>
<td>Warnings</td>
<td>Device warning message text, e.g., Low Battery</td>
</tr>
</tbody>
</table>

Provisioning Details

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

**Table 11-5  Provisioning Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Profile Applied</td>
<td>The name of the last provisioning profile that was or was not successfully applied to the device. The <strong>Provisioning Status</strong> will be either <strong>Success</strong> or <strong>Failed</strong>.</td>
</tr>
<tr>
<td>Provisioning Status</td>
<td>The device’s current provisioning status. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Clear</strong>. No provisioning has been done.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending</strong>. Provisioning is scheduled for this device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>In Progress</strong>. The device is currently being provisioned.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Success</strong>. Provisioning has been completed successfully on this device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong>. Provisioning was not completed on this device.</td>
</tr>
<tr>
<td>Pending Profile</td>
<td>The name of the provisioning profile that is scheduled to be applied to the device. In this case, the <strong>Provisioning Status</strong> will be either <strong>Pending</strong> or <strong>In Progress</strong>. This field is blank if the device is not scheduled for provisioning.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Table 11-5  Provisioning Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Attempt Date/Time</td>
<td>The date and time, in the default format of yyyy-mm-dd hh:mm:ss, of the last provisioning message exchanged with the device.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>A text description of the reason the provisioning failed. Causes for failure include:</td>
</tr>
<tr>
<td></td>
<td>• The provisioning profile does not exist</td>
</tr>
<tr>
<td></td>
<td>• The provisioning profile does not include provisioning information</td>
</tr>
<tr>
<td></td>
<td>• The CMA system no longer manages the device</td>
</tr>
<tr>
<td></td>
<td>• A password for the device is set in the video endpoint system, and you must enter it in the CMA system</td>
</tr>
<tr>
<td></td>
<td>• The device is busy</td>
</tr>
<tr>
<td></td>
<td>• A network error occurred</td>
</tr>
<tr>
<td></td>
<td>• An incomplete transfer of provisioning information occurred</td>
</tr>
<tr>
<td></td>
<td>• Provisioning has timed out</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred on the device, and you must reboot it</td>
</tr>
<tr>
<td></td>
<td>• An unknown error occurred Reboot the device.</td>
</tr>
<tr>
<td>Log Message</td>
<td>A read-only text box that contains messages related to the device provisioning status</td>
</tr>
</tbody>
</table>

**Softupdate Details**

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

**Table 11-6  Softupdate Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Softupdate Status</td>
<td>The device’s software update status. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>• Clear. A software update has not been done.</td>
</tr>
<tr>
<td></td>
<td>• Pending. A software update has been scheduled and is pending. The device may be offline or in a call.</td>
</tr>
<tr>
<td></td>
<td>• In Progress. The software update is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Success. A software update has completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Failed. A software update could not be performed.</td>
</tr>
</tbody>
</table>
### MCU Device Details

MCU device details include these fields.

**Table 11-6  Softupdate Details (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled</td>
<td>The date and time, in the default format of yyyy-mm-dd hh:mm, when the device software is scheduled to be updated. This field is blank if the device is not scheduled for provisioning.</td>
</tr>
<tr>
<td>Last Attempt Date/Time</td>
<td>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.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>A text description of the reason the software update failed. Causes for failure may include:</td>
</tr>
<tr>
<td></td>
<td>• The software update file location does not exist.</td>
</tr>
<tr>
<td></td>
<td>• A password for the device is set in the video endpoint system, and you must enter it in CMA.</td>
</tr>
<tr>
<td></td>
<td>• A network error has occurred.</td>
</tr>
<tr>
<td></td>
<td>• The update has timed out.</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred on the device, and you must reboot it.</td>
</tr>
<tr>
<td></td>
<td>• A profile has not been configured.</td>
</tr>
<tr>
<td></td>
<td>• An endpoint is offline.</td>
</tr>
<tr>
<td></td>
<td>• An incorrect activation key is in the key file.</td>
</tr>
<tr>
<td></td>
<td>• An unknown error has occurred. Reboot the device</td>
</tr>
<tr>
<td>Log Message</td>
<td>A read-only text box that contains the log message text recorded during the execution of the software update.</td>
</tr>
</tbody>
</table>

**Table 11-7  Fields in the MCU H.320 Service Dialog Box (MGC Only)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MCU H.320 Service</strong></td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td>Name of the H.320 ISDN service</td>
</tr>
<tr>
<td>Channels</td>
<td>Number of 64K channels dedicated to the MCU</td>
</tr>
<tr>
<td>Number Range</td>
<td>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).</td>
</tr>
<tr>
<td>LCR Table</td>
<td>The least-cost routing table for calls made through this gateway</td>
</tr>
</tbody>
</table>
Table 11-7 Fields in the MCU H.323 Service Dialog Box (MGC Only) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>Non-Local Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>International Prefix</td>
<td>The prefix required to dial an international number. For example, in many countries, the international prefix is 00.</td>
</tr>
<tr>
<td>Local Area Code</td>
<td>A list of local area codes, separated by commas</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority order for this service</td>
</tr>
</tbody>
</table>

Table 11-8 Fields in the MCU H.320 Service Dialog Box (MGC Only) (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The name of the H.323 service (ASCII only) defined in the MCU.</td>
</tr>
<tr>
<td>Dialing Prefix</td>
<td>Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>IP address associated with this network service and with this H.323 card in the MCU.</td>
</tr>
<tr>
<td>Alias</td>
<td>Alias for the service defined in the MCU.</td>
</tr>
<tr>
<td>Note</td>
<td>Polycom recommends using E.164 as the alias for this service.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of IP connections available.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority order for this service.</td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 6.
### Table 11-9  Fields in the MCU Gateway Service Dialog Box (MGC Only)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The name of the H.323 service defined in the MCU.</td>
</tr>
<tr>
<td>Dialing Prefix</td>
<td>Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.</td>
</tr>
<tr>
<td>H320 Service Name</td>
<td>Select a defined H320 service</td>
</tr>
<tr>
<td>Channels</td>
<td>Number of 64K channels dedicated to the MCU.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority order for this service.</td>
</tr>
</tbody>
</table>

### Table 11-10  Fields in the MGC MCU Resources Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Total Conferences</td>
<td>Maximum number of total conferences allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max CP Conferences</td>
<td>Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.</td>
</tr>
<tr>
<td>Max Total Participants</td>
<td>Maximum number of total MCU participants allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max Transcoding Ports</td>
<td>Maximum number of transcoding ports on which both ISDN and IP participants can be connected.</td>
</tr>
<tr>
<td>Total IP Parties</td>
<td>Maximum number of IP calls that can be made from this endpoint.</td>
</tr>
<tr>
<td>(Embedded MCU devices)</td>
<td></td>
</tr>
<tr>
<td>Total ISDN Parties</td>
<td>Maximum number of ISDN calls that can be made from this endpoint.</td>
</tr>
<tr>
<td>(Embedded MCU devices)</td>
<td></td>
</tr>
<tr>
<td>Total Transcoded Parties</td>
<td>Maximum number of transcoded calls (IP and ISDN calls combined) that can be made from this endpoint.</td>
</tr>
<tr>
<td>(Embedded MCU devices)</td>
<td></td>
</tr>
<tr>
<td>Use Entry Queue</td>
<td>Indicates whether the MGC device supports an IVR.</td>
</tr>
<tr>
<td>Entry Queue Number ID</td>
<td>The IP number that conference participants dial to access the IVR prompt to join a meeting.</td>
</tr>
<tr>
<td>Entry Queue ISDN Number</td>
<td>The ISDN-allocated phone number of the IVR. ISDN devices only.</td>
</tr>
</tbody>
</table>
### Table 11-11 Fields in the RMX2000 MCU Resources Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Total Conferences</td>
<td>Maximum number of total conferences allowed at once on this MCU.</td>
</tr>
<tr>
<td>Max CP Conferences</td>
<td>Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.</td>
</tr>
<tr>
<td>Max Video Ports</td>
<td>Maximum number of video ports on which participants can be connected.</td>
</tr>
<tr>
<td>Max Licensed Video Ports</td>
<td>Maximum number of total video participants allowed at once on this MCU.</td>
</tr>
<tr>
<td>Use Entry Queue</td>
<td>Indicates whether the RMX 2000 device supports an IVR.</td>
</tr>
<tr>
<td>Entry Queue Number ID</td>
<td>The IP number that conference participants dial to access the IVR prompt to join a meeting.</td>
</tr>
</tbody>
</table>

**Audio & Video Settings:** The following parameters must be set manually to synchronize with the RMX 2000 device. See the RMX 2000 documentation for more information about these settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMX API Version</td>
<td>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.</td>
</tr>
<tr>
<td>Max Voice Ports</td>
<td>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 <em>RMX 2000 Administrator’s Guide</em> for more information about this field.</td>
</tr>
<tr>
<td>Max CP Resolution</td>
<td>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 <em>RMX 2000 Administrator’s Guide</em> for more information about this field.</td>
</tr>
</tbody>
</table>

**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.
This chapter includes 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
- Roles and Permissions
- Device Associations

**Groups, Users, and User Roles**

A Polycom CMA system administrator with System Setup permissions manages users, groups, user roles, and permissions.

**Users**

**Local Users**

The Polycom CMA system allows you to add local users (i.e., users added manually to the system) and associate them with devices and roles.

For local users, the Polycom CMA system manages all user information and associations. The following table shows the user information that the Polycom CMA system maintains.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The user’s unique login name</td>
</tr>
<tr>
<td>Password</td>
<td>The user’s assigned password</td>
</tr>
<tr>
<td>First Name</td>
<td>The user’s first name</td>
</tr>
</tbody>
</table>
Enterprise Users

The Polycom CMA system can be integrated with an enterprise directory. For enterprise users, the Polycom CMA system manages only two pieces of user information: the device(s) assigned to the user and the role(s) assigned to the user. The remaining user 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 even across different domains.

When integrated with an enterprise directory, users brought into the Polycom CMA system through the enterprise directory are by default added to the system with a **Scheduler** role. This default setup allows users to log into the Polycom CMA system with their enterprise user IDs and passwords and immediately begin scheduling dial-in conferences. However, to enable dial out to enterprise users, you must associate them with devices. You can also associate enterprise users with additional roles.
Groups

Groups are efficient, because they allow you to assign roles and provisioning profiles to a set of users rather than to each user individually.

Local Groups

The Polycom CMA system allows you to add local groups (i.e., groups added manually to the system) and associate them 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.

Table 12-2  Group information

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Info</td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>A meaningful group name assigned when creating the group</td>
</tr>
<tr>
<td>Description</td>
<td>A more complete description of the group’s purpose</td>
</tr>
<tr>
<td>Directory Viewable</td>
<td>Whether or not the group is displayed in the endpoint directory</td>
</tr>
<tr>
<td>Provisioning Profile</td>
<td>The automatic provisioning profile assigned when creating the group</td>
</tr>
<tr>
<td>Associated Roles</td>
<td></td>
</tr>
<tr>
<td>Available Roles</td>
<td>The list of roles defined to the CMA system</td>
</tr>
<tr>
<td>Selected Roles</td>
<td>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 cumulative).</td>
</tr>
<tr>
<td>Group Members (Local Users Only)</td>
<td></td>
</tr>
<tr>
<td>Search Available Members</td>
<td>Search field for finding users</td>
</tr>
<tr>
<td>Search Results</td>
<td>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.</td>
</tr>
<tr>
<td>Group Members</td>
<td>The users and groups selected as part of the group</td>
</tr>
</tbody>
</table>
Enterprise Groups

The Polycom CMA system can be integrated with an enterprise directory. When 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.

For enterprise groups, the Polycom CMA system manages only three pieces of information: the provisioning profile assigned to the group, the role(s) assigned to the group, and whether or not the group is displayed in the endpoint’s directory. The remaining group information is pulled from the enterprise directory.

Roles and Permissions

The Polycom CMA system is also 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 screens and functions available to their role(s) and associated permissions. Permissions are cumulative, so users see all of the screens and functions assigned to all of their roles.

Note

Users inherit roles from their parent group(s)—local or enterprise. They cannot inherit roles from groups more distantly removed—for example, from their grandparent groups.

An administrator has three options when implementing user roles.

- Implement the system default user roles of Administrator, Operator, and Scheduler and keep the standard permissions assigned to these roles
- Implement the system default user roles of Administrator, Operator, and Scheduler but change the permissions assigned to the Operator, and Scheduler roles.
- Create unique, workflow-driven user roles and determine which permissions to assign to each user role

To ensure Polycom CMA system access and stability, the default roles cannot be deleted and the Administrator role cannot be edited.

The following table describes the standard Polycom CMA system user roles and permissions.
The following table describes the fields of the Add Role dialog box.

**Table 12-4  Fields on the Add Role Dialog Box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name (ASCII only(^a)) of the user role</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A useful description (ASCII only(^a)) of the user role</td>
</tr>
<tr>
<td>Administrator</td>
<td>Identifies which Polycom CMA system administrator screens and functions are available to the user role.</td>
</tr>
<tr>
<td>Operator</td>
<td>Identifies which Polycom CMA system operator screens and functions are available to the user role.</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Identifies which Polycom CMA system scheduling screens and functions are available to the user role.</td>
</tr>
<tr>
<td>Scheduling Level.</td>
<td>This setting determines the level of scheduling available through this role. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic.</strong> Users can schedule conferences using the conference templates defined for them. They cannot access or edit the advanced Conference Settings.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Advanced.</strong> Users can schedule conferences using the conference templates defined for them. They can also access and edit the advanced Conference Settings.</td>
</tr>
</tbody>
</table>

\(^a\) For more information, see “Field Input Requirements” on page 6.

Permissions are further associated with screens and functions. The following table describes the Polycom CMA system user interface elements related to each set of permissions.
### Table 12-5  Standard Polycom CMA Roles and Permissions

<table>
<thead>
<tr>
<th>Permission</th>
<th>Limited to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator &gt; Directory Setup</td>
<td>System Management &gt; Directory Setup &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; Dial Plan Setup</td>
<td>System Setup &gt; Dial Plan and Sites &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; Conference Setup</td>
<td>System Management &gt; Conference Setup &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; System Setup</td>
<td>System Management &gt; Dashboard &gt; All functions</td>
</tr>
<tr>
<td></td>
<td>System Management &gt; Database Backup Files &gt; All functions</td>
</tr>
<tr>
<td></td>
<td>System Management &gt; Profiles/Policies &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; System Setup</td>
<td>System Management &gt; Reports &gt; All functions</td>
</tr>
<tr>
<td></td>
<td>System Setup &gt; Server Settings &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; System Setup</td>
<td>System Setup &gt; Gatekeeper Settings &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; System Setup</td>
<td>System Setup &gt; Management &amp; Security &gt; All functions</td>
</tr>
<tr>
<td>Administrator &gt; System Setup</td>
<td>Device &gt; All functions</td>
</tr>
<tr>
<td>Operator &gt; Monitoring</td>
<td>Conference &gt; Monitor Conf View &gt; All functions (Own conferences only)</td>
</tr>
<tr>
<td></td>
<td>Device &gt; Admin/Monitor View &gt; All functions (Own devices only)</td>
</tr>
<tr>
<td>Operator &gt; Scheduling</td>
<td>Conference &gt; Monitor Conf View &gt; All functions (All conferences)</td>
</tr>
<tr>
<td>Operator &gt; Monitoring AND</td>
<td>Conference &gt; Monitor Conf View &gt; All functions (All conferences)</td>
</tr>
<tr>
<td>Operator &gt; Scheduling*</td>
<td>Device &gt; Admin/Monitor View &gt; All functions (All devices)</td>
</tr>
<tr>
<td>Operator &gt; Reports</td>
<td>System Management &gt; Reports &gt; IP Call Detail Records and ISDN Call Detail Records only</td>
</tr>
<tr>
<td>Operator &gt; Troubleshooting</td>
<td>System Management &gt; Reports &gt; Gatekeeper Message Log only</td>
</tr>
<tr>
<td>Scheduler &gt; Schedule</td>
<td>Conference &gt; Schedule Conf View &gt; All functions except Edit Conference Settings (Own conferences only)</td>
</tr>
<tr>
<td>Conferences (Basic)</td>
<td>Conference &gt; Monitor Conf View &gt; All functions (Own conferences only)</td>
</tr>
<tr>
<td>Scheduler &gt; Schedule</td>
<td>Conference &gt; Schedule Conf View &gt; All functions including Edit Conference Settings (Own conferences only)</td>
</tr>
<tr>
<td>Conferences (Advanced)**</td>
<td>Conference &gt; Monitor Conf View &gt; All functions (Own conferences only)</td>
</tr>
</tbody>
</table>

* Best practice: Use these two permission sets together
** Best practice: Create an Advanced Scheduler user role
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 cumulative; 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 cumulative; 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.

**Device Associations**

The Polycom CMA system is based on the premise that users will be associated with devices. You can associate more than one device with a user, but one device is designated as the primary device. When scheduling a user, the Polycom CMA system will, by default, schedule the user’s primary device.

The Polycom CMA system also knows the capabilities and requirements of most devices and can schedule devices accordingly.
This chapter includes information on managing users and groups within the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

- Search for a User
- Add a User
- Edit a User
- Delete a User
- Add a Local Group
- Import Enterprise Groups
- Edit a Group
- Delete a Group
- Assign Users Roles and Devices

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 field of the Users screen, search for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.
2 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.

3 If the list is too large to scan, further refine your search string.

Add a User

When you manually add a user to the Polycom CMA system, you generally add the user’s login information, assign them one or more roles to control their access to screens and functions, and associate them with one or more devices. At a minimum, you must enter their First Name or Last Name, their User ID, and their Password. When you enter the minimum information, the Polycom CMA system automatically assigns them the basic Scheduler role.

After you add a user in the Polycom CMA system, you should provide them with the following information:

• The Polycom CMA system IP address
• Their Polycom CMA system user name, password, and domain, which for enterprise users is their enterprise login credentials

To add a user

1 Go to User > Users.

2 In the User screen, click Add User.

3 Complete the General Info section of the Add New User dialog box. For more information, see Table 12-1.

4 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.
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.

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.
2. To search for a user:
   a. In the Search field of the Users screen, 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 screen 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. As required, edit the General Info, Associated Devices, and Associated Roles sections of the Edit User dialog box.
5. 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.
2. To search for a user:
   a. In the Search field of the Users screen, search for the user of interest. For example, to search for Barbara Smythe, type Bar* or *Smy* into the search field.
   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 Delete User.
4. 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. From the Groups screen, click Add Local Group.
3. Complete the General Info section of the Add Local Group dialog box. See Table 12-2.
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 From the **Groups** screen, 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*.

4 From 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 From the **Groups** screen, 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 role from a group, that role may remain associated with users in the group if at any time someone edited the user and saved the changes.

4 Click OK.

### Delete a Group

**To delete a local or enterprise group**

1 Go to **User > Groups**.
2 From the **Groups** screen, 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.

### 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:
   - In the **Search** field of the **Users** screen, type a search string. For example, to search for Barbara Smythe enter Bar* or *Smy*. 
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.

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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of the user role</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the role</td>
</tr>
</tbody>
</table>

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 screen, click Add Role.

3 Complete the Name and Description fields of the Add Role dialog box and assign permissions to the new role.
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 From 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 From 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.
This chapter describes the Polycom® Converged Management Application™ (CMA™) system Dashboard, menu, and commands. It includes these topics:

- Polycom CMA System Dashboard
- Dashboard Commands
- System Management Menu

### 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.

*Figure 14-1 Polycom CMA System Dashboard*
The Dashboard has these sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Refresh</td>
<td>By default, the system Dashboard refreshes every 5 seconds. You can change this to a value of 5 through 60. The Last Update field flashes when the system refreshes the Dashboard or when you click Refresh. If for some reason the system is unable to populate 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</td>
</tr>
<tr>
<td>MCUs</td>
<td>Displays information about the current health and status of the Polycom MCUs (MGC or RMX 2000) registered to the Polycom CMA system. The summary view displays the number of MCUs registered and whether or not any of the MCUs has errors or warnings. The detailed view identifies the MCU Name, Type, IP Address, and Status.</td>
</tr>
<tr>
<td>Devices</td>
<td>Displays information about the current health and status of the endpoints (including GW/MCU devices) registered to the Polycom CMA system. The summary view displays the number of endpoints registered and whether or not any of the endpoints has alerts or pending help requests. 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 that require attention including the device Name, Type, IP Address, and Status. Hover over the device Status to learn more about the device state.</td>
</tr>
<tr>
<td>Today's Conferences</td>
<td>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.</td>
</tr>
<tr>
<td>Scheduled Device Management</td>
<td>Displays information about the number and status of Scheduled Provisioning events and Scheduled Softupdate events. Valid states include: Pending, In Progress, Success or Failed.</td>
</tr>
<tr>
<td>Licenses</td>
<td>Displays information about the number of installed, used, and unused Polycom CMA system licenses.</td>
</tr>
</tbody>
</table>


### 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 displays the site links and network performance information for the link 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 207.

**Services** | Displays information about the service processes running on the Polycom CMA system. The summary view displays the number of **Running** and **Stopped** services. The detailed view displays a list of the service processes and **Service Name** and **Status**.

**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:

<table>
<thead>
<tr>
<th>Table 14-1</th>
<th>Dashboard Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Use this command to....</td>
</tr>
<tr>
<td>Refresh</td>
<td>Update the screen with current status</td>
</tr>
<tr>
<td>System Log Files</td>
<td>Lists the Polycom CMA system log files</td>
</tr>
<tr>
<td>Restart</td>
<td>Shuts down and restarts the Polycom CMA system. See &quot;Restart or Shut Down a Polycom CMA System&quot; on page 143.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down the Polycom CMA system. See &quot;Restart or Shut Down a Polycom CMA System&quot; on page 143.</td>
</tr>
</tbody>
</table>

System Management Menu

The System Management 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 displays these selections:

<table>
<thead>
<tr>
<th>Table 14-2</th>
<th>Dashboard Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection</td>
<td>Use this selection to...</td>
</tr>
<tr>
<td>Database Backup Files</td>
<td>View or backup the Polycom CMA system internal database backup file</td>
</tr>
<tr>
<td>Conference Setup</td>
<td>Add, edit, or delete conference templates</td>
</tr>
<tr>
<td>Directory Setup</td>
<td>Add, edit, or delete rooms to the Polycom CMA directory and to manage the Global Address Book</td>
</tr>
<tr>
<td>Profiles/Policies</td>
<td>Add, edit, or delete automatic or scheduled provisioning profiles and automatic or scheduled softupdate profiles</td>
</tr>
<tr>
<td>Reports</td>
<td>View or export system reports</td>
</tr>
</tbody>
</table>
System Management Commands

Depending on the system management selection, the Commands section may include these context-sensitive commands:

**Table 14-3  Context-sensitive System Management Menu Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Management &gt; Conference Setup &gt; Conference Templates</strong></td>
<td></td>
</tr>
<tr>
<td>Add Conference Template</td>
<td>Add a new set of conference settings designed to provide a specific conferencing experience</td>
</tr>
<tr>
<td><strong>System Management &gt; Directory Setup &gt; Rooms</strong></td>
<td></td>
</tr>
<tr>
<td>Add Room</td>
<td>Add a new conference room to the system. For administrators in the network domain, you can also use this command to select a conference room from the enterprise directory and identify it as a conference room.</td>
</tr>
<tr>
<td>Edit Room</td>
<td>Edit the information for an existing conference room</td>
</tr>
<tr>
<td>Delete Room</td>
<td>Delete a conference room from the system</td>
</tr>
<tr>
<td><strong>System Management &gt; Directory Setup &gt; GAB</strong></td>
<td></td>
</tr>
<tr>
<td>Set GAB Password</td>
<td>Set or reset the password that must be entered on the endpoint before the user can access the Global Address Book</td>
</tr>
<tr>
<td>Refresh GAB User List</td>
<td>Update the screen with current status</td>
</tr>
<tr>
<td>Add GAB User</td>
<td>Add a new entry to the Global Address Book</td>
</tr>
<tr>
<td>Edit GAB User</td>
<td>Edit the information for an existing entry in the Global Address Book</td>
</tr>
<tr>
<td>Delete GAB User</td>
<td>Delete an entry in the Global Address Book</td>
</tr>
<tr>
<td><strong>System Management &gt; Profiles/Policies &gt; Automatic Provisioning Profiles</strong></td>
<td></td>
</tr>
<tr>
<td>Add Profile</td>
<td>Add an automatic provisioning profile</td>
</tr>
<tr>
<td>Update Profile Order</td>
<td>Change the priority order for automatic provisioning profiles</td>
</tr>
<tr>
<td><strong>System Management &gt; Profiles/Policies &gt; Scheduled Provisioning Profiles</strong></td>
<td></td>
</tr>
<tr>
<td>Add Profile</td>
<td>Add a scheduled provisioning profile</td>
</tr>
<tr>
<td>Edit Profile</td>
<td>Edit an existing scheduled provisioning profile</td>
</tr>
<tr>
<td>Clone Profile</td>
<td>Copy an existing scheduled provisioning profile</td>
</tr>
<tr>
<td>Delete Profile</td>
<td>Delete an existing scheduled provisioning profile</td>
</tr>
</tbody>
</table>
### Table 14-3  Context-sensitive System Management Menu Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Use this command to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Management &gt; Profiles/Policies &gt; Automatic Software Updates</strong></td>
<td></td>
</tr>
<tr>
<td>Get Serial Numbers</td>
<td>Retrieve the serial number for the devices on which to perform a softupdate</td>
</tr>
<tr>
<td>Upload Software Update</td>
<td>Upload the softupdate package from a local computer onto the Polycom CMA system</td>
</tr>
<tr>
<td>Delete Software Update</td>
<td>Delete a softupdate package</td>
</tr>
<tr>
<td><strong>System Management &gt; Profiles/Policies &gt; Scheduled Software Updates</strong></td>
<td></td>
</tr>
<tr>
<td>Upload Software Update</td>
<td>Upload the softupdate package from a local computer onto the Polycom CMA system</td>
</tr>
<tr>
<td>Reset Software Update</td>
<td></td>
</tr>
<tr>
<td>Get Serial Numbers</td>
<td>Retrieve the serial number for the devices on which to perform a softupdate</td>
</tr>
</tbody>
</table>
This chapter describes the Polycom® Converged Management Application™ (CMA™) system management tasks. It includes these topics:

- Overview of the Polycom CMA System Database
- Connect to the Polycom CMA System Serial Console
- Backup the Polycom CMA System Database
- Copy the Polycom CMA System Database Backup Files
- Restore the Polycom CMA System Internal Databases
- Restore the Polycom CMA System External Database
- Recovery Operations - Reset First Time Setup
- Restart or Shut Down a Polycom CMA System

### Overview of the Polycom CMA System Database

Polycom CMA system information is stored in these databases:

<table>
<thead>
<tr>
<th><strong>Database</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadiManager</td>
<td>The general Polycom CMA system database that includes all data for scheduling,</td>
</tr>
<tr>
<td></td>
<td>devices, dial rules, device registration, and site topology</td>
</tr>
<tr>
<td>Logger</td>
<td>The Polycom CMA system database for call detail records and gatekeeper diagnostic</td>
</tr>
<tr>
<td>master model</td>
<td>The Polycom CMA system Microsoft MSDE system databases</td>
</tr>
<tr>
<td>msdb</td>
<td></td>
</tr>
</tbody>
</table>
The Polycom CMA system automatically optimizes its database on an ongoing basis. It backs up its internal databases daily. The backup files are stored on the CMA system hard disk.

The Polycom CMA system maintains the last four 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 139.

You can also perform manual backups and restore existing backups through the Polycom CMA system serial console or Microsoft Enterprise Manager.

You can back up databases as follow.

<table>
<thead>
<tr>
<th>From ...</th>
<th>To ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>Internal</td>
</tr>
<tr>
<td>Internal</td>
<td>External</td>
</tr>
<tr>
<td>External</td>
<td>External</td>
</tr>
</tbody>
</table>

## 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 SE200 - HyperTerminal appears.
Backup the Polycom CMA System Database

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 138.

2 From the starting menu, select (4) Database Operations.

3 From 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 139.

   – 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 screen.

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 System Management > 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 From 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 138.

2 From the **Root** menu, select **4. Database Operations**.

3 From 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 138.

2 From the **Root** menu, select **4. Database Operations**.

3 From 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 the ReadiManager and Logger databases at the same time
- Restore the ReadiManager and Logger databases from backups that were taken at the same time
- Reboot 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 Database” on page 139.
2. When the Database Operations reappears, 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 screen and the Database Operations menu reappears.
6. Repeat step 5 to restore the next database backup file.
7. After you have restored the three databases, exit the serial console and reboot 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 the three Polycom CMA database backup files as described in “Restore the Polycom CMA System Internal Databases” on page 141.

2. Run the following command using Microsoft SQL Server Management Studio or Microsoft SQL Query Analyzer.

   ```
   EXEC ReadiManager.dbo.pr_FixOrphanUsers
   ```

   **Note**
   You must have a system administrator or Polycom CMA system administrator account or the SysAdmin or db_owner role to execute this command.

3. Reboot the Polycom CMA system server.

Recovery Operations - Reset First Time Setup

To recover after a disaster, you must Reset First Time Setup. This:

- Re-enables the First Time Setup screens
- 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, you connect to the Polycom CMA serial console. Before you re-enable the First Time Setup screens, 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.
To reset First Time Setup
1. Connect to the Polycom CMA system serial console, as described in “Connect to the Polycom CMA System Serial Console” on page 138.
   The system resets itself to its first time setup state. When the reset is complete, a success message displays on the console screen.
4. Exit the serial console.
5. Review the First Time Setup screens and make required changes to any settings.
   The system is restored and is ready for use.

Restart or Shut Down a Polycom CMA System

You have three options when shutting down the Polycom CMA system.

• In emergency situations, switch off the power switch on the rear panel of the Polycom CMA system server
  Use this option only when you must immediately cut power to the server.
• 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.
  – 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 shut down a Polycom CMA system
1. (Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:
   b. Check the Conference Auto-Launch Disabled checkbox.
   c. Go to System Management > Dashboard.
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.

Disaster Recovery - Restore to Factory Default Image

In a disaster recovery situation, your Polycom Global Services 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 accompanied 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 specific to the Polycom CMA system server type: 4000 or 5000.
This chapter describes how to manage the Global Address Book and rooms in the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

- Global Address Book
- View the Global Address Book
- Add a User to the Global Address Book
- Edit a Global Address Book User
- Delete a Global Address Book User
- Edit the Global Address Book Password
- Rooms
- View the Rooms List
- Add a Room
- Edit a Room
- Delete a Room

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.
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.

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.

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.

The user information found in the Global Address Book includes:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User/Resource</td>
<td>The associated user or resource ID</td>
</tr>
<tr>
<td>Device Name</td>
<td>The name of the associated device</td>
</tr>
<tr>
<td>Type</td>
<td>The type of endpoint</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the endpoint</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number of the endpoint</td>
</tr>
<tr>
<td>Alias</td>
<td>The alias associated with this device</td>
</tr>
</tbody>
</table>
Directory Setup Operations

View the Global Address Book

To view the Global Address Book

>> Go to System Management > Directory Setup > Global Address Book.

The Global Address Book appears. It can be filtered by Address Type (Static, Dynamic, or All) or Attribute (Device Name, IP Address, or All).

Add a User to the Global Address Book

To add a user to the Global Address Book

1  Go to System Management > Directory Setup > Global Address Book.
2  From 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.
4  Click OK.

Table 16-2  Fields in the Global Address Book Entry Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name (ASCII only) of the endpoint</td>
</tr>
<tr>
<td>IP Video(H.323)</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the video endpoint system</td>
</tr>
<tr>
<td>E.164 alias</td>
<td>The alias associated with this endpoint</td>
</tr>
<tr>
<td>Rate</td>
<td>The maximum speed at which this endpoint can be</td>
</tr>
<tr>
<td></td>
<td>called</td>
</tr>
<tr>
<td>ISDN Video(H.320)</td>
<td></td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code to dial to reach the endpoint</td>
</tr>
<tr>
<td>City Code</td>
<td>The area or city code in which the endpoint is</td>
</tr>
<tr>
<td></td>
<td>located</td>
</tr>
<tr>
<td>Number A</td>
<td>The ISDN number of the endpoint</td>
</tr>
<tr>
<td>Number B</td>
<td>If the endpoint has a 2x64 ISDN line configuration, enter the second ISDN number of this endpoint</td>
</tr>
<tr>
<td>Extension</td>
<td>The extension number of the unit with gateway +</td>
</tr>
<tr>
<td></td>
<td>extension dialing</td>
</tr>
<tr>
<td>Rate</td>
<td>The maximum speed at which this unit can be</td>
</tr>
<tr>
<td></td>
<td>called</td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 6.
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 System Management > Directory Setup > Global Address Book. The Global Address Book appears. It can be filtered by Address Type (Static, Dynamic, or All) or Attribute (Device Name, IP Address, or All).

2. Select the user of interest and click Edit GAB User.

3. In the Edit GAB User dialog box, make the required changes and 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. The Global Address Book appears. It can be filtered by Address Type (Static, Dynamic, or All) or Attribute (Device Name, IP Address, or All).

2. Click the selection checkbox for the user. To delete all users, click the checkbox in the column header.

3. 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

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. Enter the new password again to confirm it and click Save.

Rooms

Only a Polycom CMA system administrator with Directory Setup permissions can view, add, edit, or delete rooms.

The following table shows the room information in the Polycom CMA system records.

Table 16-3  Room Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room Name</td>
<td>The name of the room, which appears in the address book for associated devices</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A useful description (ASCII only) of the room</td>
</tr>
<tr>
<td>Email</td>
<td>(Optional) The email address of the room administrator</td>
</tr>
<tr>
<td>Site</td>
<td>(Optional) The site in which the room is located</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Rooms and the endpoint associated with them must be assigned to the same site.</td>
</tr>
<tr>
<td>Available Devices</td>
<td>The list of unassigned devices that are managed by the CMA system</td>
</tr>
<tr>
<td>Selected Devices</td>
<td>The list of devices 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.</td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 6.
View the Rooms List

To view the Rooms list

>> Go to System Management > Directory Setup > Rooms.

The Rooms list appears. It can be filtered by Site.

Table 16-4  Information in Rooms List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
<td>The unique and required name of the room</td>
</tr>
<tr>
<td>Description</td>
<td>The optional description of the room</td>
</tr>
<tr>
<td>Associated Devices</td>
<td>The primary device associated with this room. A set of ellipses (...) indicates the room has more than one associated device.</td>
</tr>
</tbody>
</table>

Add a Room

When you add a room to the local directory, you specify settings for it and associate one or more devices with it.

If your Polycom CMA system is integrated with an LDAP directory, the directory may have rooms that are configured as users. In this case, you can search for the rooms to configure.

To add a local room

1  Go to System Management > Directory Setup > Rooms.
2  On the Rooms list, click Add Room.
   The Add New Room dialog box appears.
3  Complete the General Info and Associated Devices sections of the Add New Room dialog box. See Table 16-3.
4  Click OK.
   The new room appears in the list.

To add a room in an LDAP environment

1  Go to System Management > Directory Setup > 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 box.
3 To find a room in the LDAP directory:
   a Select the required LDAP Domain.
   b Select a Search Attribute on which to search the LDAP directory and enter a Search Value. For information on searching see “Filter and Search a List” on page 6.
   c Click Search.
      A list of the LDAP 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. See Table 16-3.
6 Click OK.
      The room is added to the Polycom CMA system.

Edit a Room

To edit a room
1 Go to System Management > Directory Setup > Rooms.
2 From 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. See Table 16-3.
4 Click OK.

Delete a Room

To delete a room
1 Go to System Management > Directory Setup > Rooms.
2 From 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.
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.

Polycom CMA system start with 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. It also enables users to request a specific bridge when scheduling a conference.

- 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.

### Table 17-1 Fields in the Add/Edit Conference Template Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A meaningful name for the template, which can be up to 32 characters long</td>
</tr>
<tr>
<td>Description</td>
<td>A description (ASCII only) of the conference settings template</td>
</tr>
<tr>
<td>Template Avail For</td>
<td>The roles to which users must be assigned to select this template when scheduling conferences</td>
</tr>
<tr>
<td><strong>Video Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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.) |
### Conference Setup Overview

#### 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 screen layout on an endpoint's monitor 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.

#### 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Mode</td>
<td>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 screen layout on an endpoint's monitor during a multipoint conference. This option requires an MCU. <strong>Note</strong> Make sure you have defined video endpoint systems and boards so that they are available for selection in continuous presence layouts.</td>
</tr>
<tr>
<td>Video Algorithm</td>
<td>Sets the compression algorithm that the MCU uses to process video. Possible values include: AUTO, H.261, H.263, H.264. The default is <strong>Auto</strong>. <strong>Notes</strong> 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</td>
</tr>
<tr>
<td>People and Content</td>
<td>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, Polycom Visual Concert PC, Polycom Visual Concert FX, DuoVideo. None is the default. <strong>Notes</strong> 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.</td>
</tr>
</tbody>
</table>
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
- The RMX 1000 system does 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**
The RMX 1000 system does 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture Mode</td>
<td>Possible values include:</td>
</tr>
<tr>
<td></td>
<td>- None. All participants see the conference in the video mode defined elsewhere.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Notes</td>
<td>Set in the RMX profile for RMX devices</td>
</tr>
<tr>
<td></td>
<td>The RMX 1000 system does not support Lecture Mode, Presentation Mode, or Lecture View Switching.</td>
</tr>
<tr>
<td>Speed</td>
<td>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.</td>
</tr>
<tr>
<td>Notes</td>
<td>This setting does not apply to Audio Only conferences.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Lecture View Switching</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>The RMX 1000 system does not support Lecture Mode, Presentation Mode, or Lecture View Switching.</td>
</tr>
<tr>
<td>High Definition</td>
<td>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.</td>
</tr>
<tr>
<td>Video Quality</td>
<td>Optimizes the video quality based on the amount of movement contained in the conference video. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>- Motion. Provides a higher frame rate without increased resolution</td>
</tr>
<tr>
<td></td>
<td>- Sharpness. Provides a higher video resolution and requires more system resources</td>
</tr>
<tr>
<td>MCU Settings</td>
<td>Specify the supported MCU types. Possible values include:</td>
</tr>
<tr>
<td>Supported MCUs</td>
<td>- MGC</td>
</tr>
<tr>
<td></td>
<td>- RMX</td>
</tr>
</tbody>
</table>
**Table 17-1 Fields in the Add/Edit Conference Template Screen (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMX Profile Name</td>
<td>Identifies the RMX profile for the conference, if the conference ends up on an RMX device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Conferences fail if they land on an RMX device and a valid RMX profile is not specified.</td>
</tr>
<tr>
<td>Always Use MCU</td>
<td>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.</td>
</tr>
<tr>
<td>Conf Settings</td>
<td></td>
</tr>
<tr>
<td>Meet Me Per Conference</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not supported on RMX devices.</td>
</tr>
<tr>
<td>Conference on Port</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not supported on RMX devices.</td>
</tr>
<tr>
<td>Conference Requires Chairperson</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>H.243 cascade control allows the MGC-50 or MGC-100 to support a cascading configuration of conferences with the capabilities of H.243.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> • Set in the RMX profile for RMX 2000 devices • The RMX 1000 system does not support the <strong>Chairperson</strong> feature.</td>
</tr>
<tr>
<td>Entry Tone</td>
<td>Sets an entry tone sound when a participant enters a conference.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not user-configurable for RMX devices</td>
</tr>
<tr>
<td>Exit Tone</td>
<td>Sets an exit tone sound when a participant leaves a conference.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not user-configurable for RMX devices</td>
</tr>
<tr>
<td>End Time Alert Tone</td>
<td>Sets an alert tone to sound near the end of the conference.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not user-configurable for RMX devices</td>
</tr>
</tbody>
</table>
### Table 17-1  Fields in the Add/Edit Conference Template Screen (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Talk Hold Time (sec)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Not user-configurable for RMX devices</td>
</tr>
<tr>
<td>End Time Alert (minutes)</td>
<td>Specifies the number of minutes before the conference end that the End Time Alert Tone should sound.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Not user-configurable for RMX devices</td>
</tr>
<tr>
<td>T120 Rate</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Because this setting uses resources on the MCU device, it is recommended that you select <strong>None</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Not supported on RMX devices</td>
</tr>
<tr>
<td>Audio Algorithm</td>
<td>Sets the compression algorithm that the MGC uses to process audio. The default is <strong>Auto</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Not user-configurable for RMX devices</td>
</tr>
<tr>
<td>Audio Mix Depth (sites)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Not user-configurable for RMX devices</td>
</tr>
</tbody>
</table>

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

**Note**

Third-party MCUs are not supported in Polycom CMA scheduling. 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:

Table 17-2 Fields in the Conference Settings Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Auto Launch</td>
<td>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 the restart or shutdown.</td>
</tr>
<tr>
<td>Conference Time Warning</td>
<td>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.</td>
</tr>
</tbody>
</table>
| SE200-generated Emails | Specifies information the Polycom CMA system uses to send conference email notifications.  
  - From Address. Specify the email account (ASCII only) from which the Polycom CMA system will send conference notification emails.  
  - SMTP Server. Specify the IP address of the mail server from which the Polycom CMA system will send conference notification emails.  
  By default, the Polycom CMA system emails are addressed as PanAlert@vtcmanager.com. |

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.

a. For more information, see “Field Input Requirements” on page 6.
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
• Add a Conference Template
• Edit a Conference Template
• Delete a Conference Template
• Set Conference Settings
• Disable Conference Auto-Launch
• Disable Conference Time Warning
• Edit the Polycom CMA System Email Account

**View the Conference Templates List**

To view the Conference Template list

>> Go to System Management > Conference Setup > Conference Templates.

The Conference Templates list appears.

**Add a Conference Template**

To add a conference template

1 Go to System Management > Conference Setup > Conference Templates.
2 On the Conference Templates list, click Add Conference Template.
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 System Management > Conference Setup > Conference Templates.
2 On the Conference Templates list, select the template of interest and click Edit Conference Template.
3 Edit the General Info, Video Settings, MCU Settings, and Conf Settings sections of the Add Conference Template dialog box as required.
4 Click OK.

Delete a Conference Template

To delete a conference template
1 From the Conference Setup menu, choose Conference Templates.
2 Select the template or templates you want to delete, and then click Delete.
3 Click Yes to confirm the deletion.
Set Conference Settings

To specify conference settings
2. When the Conference Settings screen appears, make the required selections.
3. Click Update.

Disable Conference Auto-Launch

To disable conference auto-launch
2. In the Conference Auto-Launch section of the Conference Settings screen appears, check the Disable checkbox.
3. Click Update.

Disable Conference Time Warning

To disable the conference time warning
2. In the Conference Auto Launch section of the Conference Settings screen appears, uncheck the Enabled checkbox.
3. Click Update.

Edit the Polycom CMA System Email Account

To edit the Polycom CMA system email account
2. In the System-generated Emails section of the Conference Settings screen appears, enter the required From Address and SMTP Server IP.
3. Click Update.
This chapter describes how to view and export reports available for the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

- Gatekeeper Message Log
- Site Statistics
- Site Link Statistics
- Call Detail Record Reports
- Conference Summary Reports
- System Log Files

**Gatekeeper Message Log**

Use the **Gatekeeper Message Log** screen 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
The Gatekeeper Message Log has these fields:

**Table 19-1 Information on Gatekeeper Message Log**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>These types of messages display:</td>
</tr>
<tr>
<td></td>
<td>• Information, which indicates normal communications between the Polycom CMA</td>
</tr>
<tr>
<td></td>
<td>system and the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Warning, which indicates an unscheduled call and the inability to assign</td>
</tr>
<tr>
<td></td>
<td>E.164 and ISDN numbers to an endpoint.</td>
</tr>
<tr>
<td></td>
<td>• Error, which indicates the registration of an endpoint or a call failed,</td>
</tr>
<tr>
<td></td>
<td>or a lack of resources for this gateway or MCU exists.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time of the event.</td>
</tr>
<tr>
<td>Category</td>
<td>Specifies whether an event is a registration, call, or neighboring gatekeeper request.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the message sent to or received from the endpoint, identified by the IP address.</td>
</tr>
</tbody>
</table>

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 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
2. Use the Filter on the Gatekeeper Message Log list to customize the list.
3. Select the message of interest.
   The Call Details box is populated with the message information.
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
2. When the Gatekeeper Message Log screen 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
2. When the Gatekeeper Message Log screen appears, click Clear Events.
3. Click Yes to confirm the action.
   The Gatekeeper Message Log is cleared.
**Pause and Restart Logging**

**To pause logging**

2. When the Gatekeeper Message Log screen 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.

**Site Statistics**

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.

**View Site Statistics**

**To view Site Statistics**

1. Go to System Management > 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. From the Site Name list, select the site(s) to chart.
   c. From 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

Use the Site Link Statistics report to check call rate and call quality statistics for the defined site links.

View Site Link Statistics

To view Site Link Statistics

1. Go to System Management > 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. From the Site Name list, select the site(s) to chart.
   c. From 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 screens provide call detail record (CDR) information: CDR Table: IP View and CDR Table: ISDN View. You can view CDR reports and export them as comma-separated value (CSV) files to spreadsheet programs, such as Microsoft Excel.

The CDR report automatically lists all IP or ISDN calls made to or from every device for the current date. Using the Filter by: drop-down list, you can filter the list by date, time, device type, IP address, and system to show a specific set of call data. To view the complete CDR report select Clear Filter from the Filter by: list.

The following tables describe the fields of the IP and ISDN Call Detail Record Reports.
### Table 19-2  Information in the CDR Table - IP View Screen  Fields of the IP Call Detail Record Reports

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call ID</td>
<td>ID automatically generated for the call.</td>
</tr>
<tr>
<td>Conf ID</td>
<td>The GUID (global unique identifier) for the conference.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time the call started, provided in local time for the server.</td>
</tr>
<tr>
<td>Source</td>
<td>Name, IP, or alias of the device that originated the call.</td>
</tr>
<tr>
<td>Source Address</td>
<td>IP address of the device that originated the call.</td>
</tr>
<tr>
<td>Destination</td>
<td>Name, IP address, or alias of the device that received the call.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>IP address of the device that received the call.</td>
</tr>
<tr>
<td>Call Type</td>
<td>The type of call: scheduled or unscheduled.</td>
</tr>
<tr>
<td>Bandwidth (Kbps)</td>
<td>Bandwidth that was used for the call.</td>
</tr>
<tr>
<td>Duration (min)</td>
<td>Length of the call in minutes, up to a maximum of 999.</td>
</tr>
<tr>
<td>Q.850 Code</td>
<td>Standard Q.850 cause code for call termination.</td>
</tr>
</tbody>
</table>

### Table 19-3  Information in the CDR Table - ISDN View Screen Fields of the ISDN Call Detail Record Reports

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call ID</td>
<td>ID automatically generated for the call.</td>
</tr>
<tr>
<td>Conf ID</td>
<td>The alphanumeric value that identifies the conference.</td>
</tr>
<tr>
<td>Note</td>
<td>This value is only available for multipoint conferences.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time the call started, provided in local time for the server.</td>
</tr>
<tr>
<td>System Name</td>
<td>Name, IP, or alias of the device that originated the call.</td>
</tr>
<tr>
<td>Remote Site</td>
<td>Name, IP, or alias of the device that received the call.</td>
</tr>
<tr>
<td>Direction</td>
<td>Indicates whether the call was inbound or outbound.</td>
</tr>
<tr>
<td>Call Type</td>
<td>The type of call: scheduled or unscheduled.</td>
</tr>
<tr>
<td>Bandwidth (Kbps)</td>
<td>Bandwidth that was used for the call.</td>
</tr>
<tr>
<td>Duration (min)</td>
<td>Length of call in minutes, up to a maximum of 999.</td>
</tr>
<tr>
<td>Cause Code</td>
<td>Standard Q.850 cause code for call termination.</td>
</tr>
</tbody>
</table>
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.

### View and Export the IP Call Detail Records

**To view and export the IP Call Detail Records**

1. Go to **System Management > Reports > IP Call Detail Records**.
   
   The **IP Call Detail Records** list appears. The calls are listed in order of date and time, with the earliest call shown first.

**Note**
IP calls through the Global Address Book that are not registered to the gatekeeper do not display in this report.

2. Use the **Filter** on the **IP Call Detail Records** list to customize the list by **Date**, **IP Address**, **Device Type**, **Call Type** and **Duration**.

3. To export the report:
   
   a. Click **Export**.
   
   b. From the **File Download** dialog box, click **Save**.
   
   c. In the **Save As** dialog box, browse to a location and click **Save**.

### View and Export the ISDN Call Detail Records

**To view and export the ISDN Call Detail Records**

1. Go to **System Management > Reports > ISDN Call Detail Records**.
   
   The **ISDN Call Detail Records** list appears. The calls are listed in order of date and time, with the earliest call shown first.

2. Use the **Filter** on the **ISDN Call Detail Records** list to customize the list by **Date**, **System Name**, **Device Type**, **Call Type** and **Duration**.

3. To export the report:
   
   a. Click **Export**.
   
   b. From the **File Download** dialog box, click **Save**.
In the **Save As** dialog box, browse to a location and click **Save**.

## Conference Summary Reports

Use the **Conference Summary Report** option to review monthly summary information about past Polycom CMA system conferences. These reports may be helpful in understanding and optimizing your conferencing system usage and creating useful Polycom CMA system templates and RMX 2000 profiles.

The following tables describe the fields of the Conference Summary Report.

### Table 19-4  Information in the Conference Summary Report Fields of the Conference Summary Report

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Information is displayed on a month-by-month basis and an average for the selected months</td>
</tr>
<tr>
<td>Scheduled Conf's</td>
<td>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)</td>
</tr>
<tr>
<td>Adhoc Conf's</td>
<td>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</td>
</tr>
<tr>
<td>MP Conf's</td>
<td>The number of multipoint conferences scheduled using one of the Polycom CMA system scheduling interfaces</td>
</tr>
<tr>
<td>P2P Conf's</td>
<td>The number of point-to-point conferences scheduled using one of the Polycom CMA system scheduling interfaces</td>
</tr>
<tr>
<td>Gateway Conf's</td>
<td>The number of scheduled conferences that used a gateway to reach one or more devices</td>
</tr>
<tr>
<td>Embedded MP Conf's</td>
<td>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</td>
</tr>
<tr>
<td>P2P Conf's on MCU</td>
<td>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</td>
</tr>
<tr>
<td>Short Conf's</td>
<td>The number of scheduled conferences that were scheduled to last 30 minutes or more, but which actually lasted less than 30 minutes</td>
</tr>
</tbody>
</table>
In addition, you can create graphical reports for the following conference data.

**Table 19-4  Information in the Conference Summary Report (continued)**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Minutes</td>
<td>The sum of the scheduled minutes for all Polycom CMA system scheduled conferences</td>
</tr>
<tr>
<td>Executed Minutes</td>
<td>The sum of the actual minutes for all Polycom CMA system scheduled conferences</td>
</tr>
<tr>
<td>Total Parts</td>
<td>The sum of the participants that joined Polycom CMA system scheduled conferences</td>
</tr>
<tr>
<td>Avg Parts in MP Confns</td>
<td>The average number of participants that joined scheduled Polycom CMA system multipoint conferences</td>
</tr>
</tbody>
</table>

**To create a Conference Summary Report**

2. As needed, change the **From:** and **To:** dates to select the date range for the report, and click **View**.
3. To create one of the conference summary report charts, click the chart name.
4. To export the report:
   a. Click **Export**.
   b. From the **File Download** dialog box, click **Save**.
   c. In the **Save As** dialog box, browse to a location and click **Save**.
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.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Files Related to Basic System Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>SE200MasterService.txt</td>
<td>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</td>
</tr>
<tr>
<td>SE200SerialConsoleLog.txt</td>
<td>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.</td>
</tr>
<tr>
<td>ESINSTALL-&lt;timestamp&gt;.txt</td>
<td>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</td>
</tr>
<tr>
<td>ESUPGRADE-&lt;timestamp&gt;.txt</td>
<td>Log file that shows the output of the Polycom CMA system upgrade script (not applicable unless an upgrade was performed)</td>
</tr>
<tr>
<td><strong>Log File Related to Dial Plan Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>DialRule_Log.txt</td>
<td>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.</td>
</tr>
<tr>
<td>SiteTopo_Log.txt</td>
<td>When in debug mode, this log file contains messages about site topology entry and usage.</td>
</tr>
<tr>
<td><strong>Log File Related to External Database Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>ServiceMonitor_Log.txt</td>
<td>Log file for the redundancy service that shows when a redundant Polycom CMA system goes into active or standby mode</td>
</tr>
<tr>
<td><strong>Log Files Related to Scheduling Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>AdapterLog_SCH.txt</td>
<td>.NET remoting log file that shows low-level communication errors between internal system components--in this case, the scheduling component</td>
</tr>
<tr>
<td><strong>Log Files Related to Global Address Book Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>AdapterLog_GAB.txt</td>
<td>.NET remoting log file that shows low-level communication errors from the GAB communications with the integration layer</td>
</tr>
<tr>
<td>ComponentLog_GAB.txt</td>
<td>.NET remoting log file that shows low-level communication errors from the GAB communications with devices</td>
</tr>
<tr>
<td>EXXX_LOGx.txt</td>
<td>Log files for web services, device manager, and conference monitoring.</td>
</tr>
</tbody>
</table>
### Table 19-5  Polycom CMA System Log Files

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log Files Related to Device Management Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>AdapterLog_GMS.txt</td>
<td>.NET remoting log file that shows low-level communication errors between internal system components—in this case, the management component</td>
</tr>
<tr>
<td>&lt;DeviceType&gt;Device.txt</td>
<td>Log file that captures device specific message</td>
</tr>
<tr>
<td>&lt;DeviceType&gt;DeviceCollection.txt</td>
<td>Log file that captures device specific message</td>
</tr>
<tr>
<td>&lt;DeviceType&gt;PasswdErrs.log</td>
<td>Log file that captures device specific messages related to potential password mismatches</td>
</tr>
<tr>
<td>DeviceManager.txt</td>
<td>Log file for the device management process</td>
</tr>
<tr>
<td>DeviceManagerService.txt</td>
<td>Log file for the device management process</td>
</tr>
<tr>
<td>SoftUpdate</td>
<td>Log file that shows when a device is updated with a new software package via a scheduled softupdate</td>
</tr>
<tr>
<td><strong>Log Files Related to Gatekeeper Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>AdapterLog_PN.txt</td>
<td>.NET remoting log file that shows low-level communication errors between internal system components—in this case, the gatekeeper component</td>
</tr>
<tr>
<td>PN_Log.txt</td>
<td>General gatekeeper log file</td>
</tr>
<tr>
<td>MQM_Log.txt</td>
<td>General media quality monitor log file that will show any errors when writing CDRs or media quality data to the database</td>
</tr>
<tr>
<td><strong>Log Files Related to Call Management Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>Messages.txt</td>
<td>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.</td>
</tr>
<tr>
<td>CS_&lt;conf_name&gt;.txt</td>
<td>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_&lt;conf_name&gt;, where &lt;conf_name&gt; is the name of the scheduled conference. This is always on, and there is no logging level.</td>
</tr>
<tr>
<td><strong>Log Files Related to Web Services Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>apache_access.log.&lt;xxxx&gt;</td>
<td>Apache web server access log that shows when and what url was requested</td>
</tr>
<tr>
<td>apache_error.log</td>
<td>Log file that captures error messages from the Apache web server</td>
</tr>
<tr>
<td>mod_jk.log</td>
<td>Log file that shows which web requests were forwarded from Apache web server to the Tomcat servlet engine.</td>
</tr>
<tr>
<td><strong>Log Files Related to Presence Functionality</strong></td>
<td></td>
</tr>
<tr>
<td>Jserver.log.&lt;n&gt;</td>
<td>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.</td>
</tr>
</tbody>
</table>
To view System Log Files

   
   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 log file in .txt format:
   
   a. Select the log file of interest.
   
   b. Click Save.
   
   c. In the Save As dialog box, browse to a location and click Save.

Change the System Log Level

To edit the current system log level


   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

### Polycom CMA System Log Files

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot.log</td>
<td>JBoss startup log. JBoss is the container service for the Jserver service</td>
</tr>
<tr>
<td>debug.log</td>
<td>Openfire debug log that shows errors related to connection to internal LDAP</td>
</tr>
<tr>
<td>error.log</td>
<td>Openfire error log</td>
</tr>
<tr>
<td>info.log</td>
<td>Openfire information log</td>
</tr>
<tr>
<td>warn.log</td>
<td>Openfire warning log</td>
</tr>
<tr>
<td>openfire.log</td>
<td>Openfire service log that shows when Openfire was started and problems</td>
</tr>
<tr>
<td></td>
<td>related to its startup</td>
</tr>
</tbody>
</table>

Table 19-5 Polycom CMA System Log Files
- Warn
- Error
- Major
- Fatal
- Off

3 In a redundant configuration, repeat steps 1 and 2 on the redundant server.
This chapter provides an overview of the Polycom® Converged Management Application™ (CMA™) System Setup menu. It includes these topics:

- System Setup Menu
- Overview of Site Topology
- Site Topology and Site Link Examples
- Default Polycom CMA System Dial Plan Settings
- Polycom CMA System LDAP Integration

**System Setup Menu**

The System Setup 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 System Setup menu includes these items:

**Table 20-1  System Management Menu**

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Settings</td>
<td>These selections for the server, network, database, and directory service are entered during the Polycom CMA system First Time Setup process and do not change frequently. Use the Server Settings option, when you do need to change them.</td>
</tr>
</tbody>
</table>
Overview of Site Topology

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.

### Table 20-1 System Management Menu

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
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 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.

**Site Topology and Site Link Examples**

Two examples of site links follow: a simple, direct link and a complex,
multisite link.

Figure 20-1 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 20-1  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 20-2 shows the same Company ABC with two additional sites in Paris and Tel Aviv.

*Figure 20-2 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

**Table 20-2 Site Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Site Name</td>
<td>The physical location of the site. The name can be up to 32 characters long, and may include spaces, dashes, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII only) of the site.</td>
</tr>
<tr>
<td>Override ITU Dialing Rules</td>
<td>Check this box to override the standard dialing rules established by the International Telecommunications Union.</td>
</tr>
<tr>
<td>PBX Access Code</td>
<td>The access code required to enter the site’s PBX system.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code for the country in which the site is located.</td>
</tr>
<tr>
<td>Area Code</td>
<td>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.</td>
</tr>
<tr>
<td># of Digits in Subscriber Number</td>
<td>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.</td>
</tr>
<tr>
<td>Default LCR Table</td>
<td>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.</td>
</tr>
<tr>
<td>Assignment Method</td>
<td>The ISDN number assignment method for the site. Possible values include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>No Auto Assignment.</strong> Select this option when ISDN numbers are not assigned to IP devices.</td>
</tr>
<tr>
<td></td>
<td>- <strong>DID (Direct Inward Dial).</strong> Select this option when you assign a range of phone numbers received from the telephone company service.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Gateway Extension Dialing.</strong> 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.</td>
</tr>
</tbody>
</table>

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.

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

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 V2IU 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 V2IU appliance) code before the IP address in the dial string.
System Setup Overview

Table 20-2  Site Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Signaling Address</td>
<td>IP address of the SBC or ALG server. Supports only IPv4</td>
</tr>
<tr>
<td>Port</td>
<td>Port address of SBC or ALG server</td>
</tr>
<tr>
<td>Site Subnet</td>
<td></td>
</tr>
<tr>
<td>Subnet IP Address/Mask</td>
<td></td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 7.

Site Link Settings

Table 20-3  Fields on the Link Editor Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Name</td>
<td>Name (ASCII onlya) of the inter-site link</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII onlya) of the inter-site link</td>
</tr>
<tr>
<td>From Site</td>
<td>Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.</td>
</tr>
<tr>
<td>To Site</td>
<td>Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet or VPN option.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Specifies a direct link between two physical sites or a multisite link, for which a path of links is defined</td>
</tr>
<tr>
<td>Bandwidth (Kbps)</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Bit Rate (Kbps)</td>
<td>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.</td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 7.

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 ReadiVoice 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 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.

---

**Gatekeeper Overview**

During the **First Time Setup** procedure, the Polycom CMA system is automatically designated as the primary gatekeeper and the default gatekeeper settings are implemented.

Use the **Gatekeeper Settings** menu to change the primary gatekeeper settings, add an alternate gatekeeper, or add neighboring gatekeepers.

An alternate gatekeeper ensures endpoint availability. Endpoint remain registered with the alternate gatekeeper unless it goes down. Endpoints then can register with the gatekeeper that has the highest priority that can respond to the registration request.

You may also create additional, neighboring gatekeepers to enable routing of H.323 calls to neighboring gatekeepers.

**Note**
A neighboring H.323 gatekeeper may require additional configuration to completely integrate with the Polycom CMA gatekeeper. Also, not all Polycom CMA system parameters correspond to parameters on a neighboring gatekeeper.
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 neighboring gatekeepers for resolution. To enable call forwarding, create a neighboring gatekeeper and a dialing rule that routes calls using a particular prefix to the neighboring region. Be sure not to use a prefix that already routes calls to a dial plan service such as Simplified Dialing.

If you have a Polycom PathNavigator installed, it can act as a neighboring gatekeeper to the Polycom CMA system.

**Note**

To prevent a site from participating in a dial plan, do not assign it to a region.

For more information about the different gatekeepers, see:

- Primary Gatekeeper Settings
- Alternate Gatekeeper Settings

### Primary Gatekeeper Settings

**Primary Gatekeeper Settings** affect how devices register and calls are made in the video communications network. The Primary Gatekeeper Settings:

- Identify the primary gatekeeper
- 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 rogue (unregistered) endpoints

The **Primary Gatekeeper Settings** include these fields:

#### Table 20-4  Fields in Primary Gatekeeper Settings screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper Identifier</td>
<td>The gatekeeper identifier (ASCII-only) 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.</td>
</tr>
<tr>
<td>Gatekeeper Description</td>
<td>The description (ASCII only) of this gatekeeper on the network</td>
</tr>
<tr>
<td>Default Gatekeeper</td>
<td>Select this check box to identify the default gatekeeper to endpoints seeking registration OR select this check box to enable automatic registration when you have more than one gatekeeper on the network. <strong>Note</strong> To register an MGC-50 or MGC-100 with CMA, you must select this check box.</td>
</tr>
</tbody>
</table>
### Table 20-4  Fields in Primary Gatekeeper Settings screen (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Registration of</td>
<td>Informs the gatekeeper of which endpoints to register.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All Endpoints</strong>. 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Predefined Endpoints Only</strong>. With this secure gatekeeper policy, devices are automatically added to the device list via the Global Address Book.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Endpoints in Defined Sites</strong>. With this moderately open registration policy, devices at identified Polycom CMA system sites may automatically register with the Polycom CMA system.</td>
</tr>
<tr>
<td>Registration Timeout (day)</td>
<td>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.</td>
</tr>
<tr>
<td>Registration Refresh (seconds)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If the endpoint responds with a registration request message, the endpoint is online. If not, the endpoint is offline.</td>
</tr>
<tr>
<td></td>
<td>When the endpoint is registered to another gatekeeper, the Polycom CMA system still shows the endpoint’s status.</td>
</tr>
<tr>
<td></td>
<td>To view the endpoint’s state (<strong>Online</strong> or <strong>Offline</strong>), go to <strong>Device &gt; Admin/Monitor View</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Endpoints are <strong>Offline</strong> when they have been turned off or have been removed from the network. Endpoints return to an <strong>Online</strong> state when they have been turned on or have reregistered with Polycom CMA system.</td>
</tr>
<tr>
<td>Maximum Neighbor Gatekeeper Hop Counts</td>
<td>Limits the number of connections to make when an endpoint seeks dialing resolution. The default is 3.</td>
</tr>
<tr>
<td>Log calls to/from unregistered endpoints</td>
<td>Logs calls to and from rogue endpoints. To view call logs, select <strong>System Management &gt; Reports &gt; Gatekeeper Message Log</strong>.</td>
</tr>
<tr>
<td>Deny calls to/from unregistered endpoints</td>
<td>Prevents calls to and from rogue endpoints.</td>
</tr>
<tr>
<td>IRR frequency</td>
<td>The frequency of the gatekeeper’s response to the calling or receiving endpoint. The default is 0.</td>
</tr>
</tbody>
</table>
Alternate Gatekeeper Settings

Alternate Gatekeeper Settings affect how devices register with the alternate gatekeeper when the primary gatekeeper cannot respond to a request. These settings:

- Identify the alternate gatekeeper
- Identify the port the alternate gatekeeper uses to communicate with the endpoints

Note
An alternate gatekeeper is not a redundant gatekeeper.

Use the Alternate Gatekeeper screen to enter information about an alternate gatekeeper that devices can use when the primary gatekeeper (the Polycom CMA system) cannot respond to a request.
The **Alternate Gatekeeper Settings** include these fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to Register</td>
<td>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.</td>
</tr>
<tr>
<td>Alternate Gatekeeper ID</td>
<td>The alternate gatekeeper’s network identifier (ASCII only)</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the alternate gatekeeper</td>
</tr>
<tr>
<td>Port</td>
<td>The port number (usually 1719) that the alternate gatekeeper uses to communicate with endpoints</td>
</tr>
<tr>
<td>Priority</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

**Redundant Polycom CMA 5000 System Configuration**

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 or server reboot.

• 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. Documented procedures for redundancy include:

- “Configure Redundancy” on page 10
- “Configure the External Database for Redundancy” on page 10
- “Set the Virtual IP Address for the Redundant System” on page 11
- “To license a redundant Polycom CMA 5000 system” on page 12
- “Implement a Redundant Polycom CMA 5000 System” on page 203
- “Failover to a Redundant Polycom CMA 5000 System Server” on page 205
- “Discontinue a Redundant CMA 5000 System Configuration” on page 205
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 Polycom CMA System Time Settings
- Integrate the Polycom CMA System to an External Database
- Revert the Polycom CMA System to the Internal Database
- Integrate the Polycom CMA System to an Enterprise Server
- Add Polycom CMA System Licenses
- Implement a Redundant Polycom CMA 5000 System
- Failover to a Redundant Polycom CMA 5000 System Server
- Add Your Own Logo to the Polycom CMA System User Interface
- Add Your Own Logo to the Polycom CMA Desktop User Interface

## 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The NetBIOS name (ASCII only) of the Polycom CMA server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The static IP address for the Polycom CMA server</td>
</tr>
</tbody>
</table>
To edit the Polycom CMA system network settings

1. Go to System Setup > Server Settings > Network.
2. On the Network screen, make the required changes. See Table 21-1.
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.

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:

**Table 21-2  System Time Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Time Zone</td>
<td>The time zone in which the Polycom CMA server resides</td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving?</td>
<td>Select this checkbox to adjust the clock automatically for daylight savings time.</td>
</tr>
<tr>
<td>Use Current Time</td>
<td>Select this checkbox to input the current date and time.</td>
</tr>
</tbody>
</table>

**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.
To edit the Polycom CMA system time settings

1. Go to **System Setup > Server Settings > System Time**.
2. On the **System Time** screen, make the required changes. See Table 21-2.

### 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 reboot the Polycom CMA system to ensure the time is synchronized correctly.

3. Click **Update**.

### Table 21-2  System Time Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Date</td>
<td>The system date for the Polycom CMA system</td>
</tr>
<tr>
<td>Current Time</td>
<td>The system time for the Polycom CMA system</td>
</tr>
<tr>
<td>Use External NTP Server Time</td>
<td>Select this checkbox to synchronize the Polycom CMA system date and time with an external NTP server.</td>
</tr>
<tr>
<td>Synchronization</td>
<td></td>
</tr>
<tr>
<td>IP address or DNS resolved name</td>
<td>The IP address or fully qualified domain name (ASCII only) of the NTP server</td>
</tr>
<tr>
<td>Minutes between synchronization</td>
<td>Input how often the Polycom CMA system should synchronize with the NTP server</td>
</tr>
<tr>
<td>attempts</td>
<td>The default is 60 minutes.</td>
</tr>
</tbody>
</table>

a. For more information on field limitations, see “Field Input Requirements” on page 6.
Integrate the Polycom CMA System to an External Database

To integrate the Polycom CMA system to an external Microsoft SQL Server, edit the Database Integration server setting.

Notes
- Polycom CMA 5000 systems require an external database. We recommend implementing an external database if your Polycom CMA 4000 system has 100+ registered endpoints.
- 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 System Setup > Server Settings > Database.
2. On the Database screen, select the Use an external SQL Server database check box.
3. Click Database Setup and download the Remote Database Setup Utility, DBSetup.exe, to your computer.
4. Run the Remote Database Setup Utility and complete the information requested in the setup screens.
   - 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.

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.

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.

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.

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.

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.

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.
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 screen. (Note that the database instance name field is ASCII only; for more information on field limitations, 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 System Setup > Server Settings > Database.

2 On the Database screen, deselect the Use an external SQL Server database check box and click Update.

Note
To revert back to the external database, follow the procedure to “Integrate the Polycom CMA System to an External Database” on page 198, 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 Server

To allow Polycom CMA system users who enter their standard network usernames and passwords to log into the Polycom CMA system and 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 CMA system and access CMA services such as automatic provisioning, automatic softupdate, and presence, see “Enable an Active Directory Domain Controller” on page 200.

The Polycom CMA system requires a login 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 System Setup > Server Settings > LDAP.
2 On the LDAP screen, check **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 on field limitations, see “Field Input Requirements” on page 6.

4 Enter the **LDAP User ID** and **Password** required to access the LDAP server and click **Update.**

**Notes**
- This User ID must have read access to all of the domains the LDAP server.
- This User ID is automatically associated to a Polycom CMA Administrator role.

---

**Enable an Active Directory Domain Controller**

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, you must integrate the Polycom CMA system with your Active Directory domain controller.

The Polycom CMA system requires an account that has read access to all domains in the Active Directory.

**Note**
To allow Polycom CMA system users who enter their standard 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 Server” on page 199.

**To enable an active directory domain controller**

1 Go to **System Setup > Server Settings > LDAP.**

2 On the LDAP screen, check **Enable Active Directory Domain Controller.**

3 Enter the IP address for the **Active Directory Domain Controller.**

4 Click **Update.**
Add Polycom CMA System Licenses

A Polycom CMA 5000 system seat capacity scales from 200 to 5,000 devices depending on the model selected. The entry-level platform comes preconfigured with a baseline capacity of 200 or 500 client access licenses. Additional licensing is offered in the following expansion license pack sizes: 100/500/1000.

When applied to the system, an expansion license pack augments the device license count. For example, applying a 100-device expansion license pack to a baseline system will yield a total license count of 300 concurrent licenses.

Where applicable, the number of concurrent calls supported by a Polycom CMA 5000 system is derived from the number of device licenses at a 1500/5000 ratio (call/devices). For example, a system licensed for 5000 devices supports up to 1500 concurrent calls in routed mode, 3000 calls in direct mode.

A Polycom CMA 4000 system capacity scales from 25 devices up to 400 devices. The system comes preconfigured with a baseline capacity of 25 devices. Additional device licensing is offered in the following expansion license pack sizes: 25/100/250.

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). The exception is the 25-device baseline system, which supports up to 12 concurrent calls. As an example, a system licensed for 100 devices supports up to 30 concurrent calls, while a 400-device licensed system supports up to 100 concurrent calls.

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.

Licenses consumed by a Polycom CMA Desktop client are automatically released after a set number of days of inactivity. Seats consumed by a registered device are never automatically freed-up. An administrator must manually delete the device from the system to free up the license.

System administrators and end-users do NOT consume a device license.

The initial Polycom CMA system includes a trial license for 25 seats, which allows you to start using the system immediately. The trial license is valid for up to 60 days, starting from the date of first-time setup.

You should receive one or more License Certificates, according to your order. You must activate each License Certificate to receive an activation key, which you enter in the Polycom CMA system.

Note
Installation of a new license key completely and immediately replaces the functionality provided by the existing license key.
So licensing your Polycom CMA system is a two step process:

- Request a Software Activation Key.
- Enter the Polycom CMA System License Number

These steps are described in the following sections.

**Request a Software Activation Key**

**To request a software activation key**

1. Go to System Setup > Server Setup > Licenses and record the Polycom CMA server serial number:

   _______________________

3. Log in or create a New User Account.
4. Select Product Activation.
5. Enter the software license number listed on your License Certificate and the serial number you recorded in step 1.
6. Click Generate.
7. When the activation key appears, record it:

   __________-__________-__________-__________

8. Repeat this procedure for each additional license key required.

**Enter the Polycom CMA System License Number**

**To enter the Polycom CMA license number**

2. Enter the new license number 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
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. To reclaim licenses more slowly, increase the threshold.
3. Click Update.

The license number appears in the list and the number of active licenses is updated.

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. For information on installing a new redundant Polycom CMA 5000 system, see the CMA Getting Started Guide and follow up with “Configure Redundancy” on page 163.

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” on page 202.
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 198.
5. On the primary server:
   a. Go to System Setup > Server Settings > Redundant Configuration.
If the two CMA systems are installed and configured correctly on the network, both servers are displayed in the **Redundant Configuration** screen.

b Enter the **Virtual IP** for the redundant system and click **Submit**.

6 On the redundant server:

a Go to **System Setup > Server Settings > Database**.

b On the **Database** screen, 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** screen. (Note that the **Database Instance Name** field is ASCII only; for more information on field limitations, see “Field Input Requirements” on page 6.)

d Click **Update**.

The Polycom CMA 5000 system connects to the database server and the redundant server reboots 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 205.

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 **System Setup > Server Setup > 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 **System Management > Dashboard > Restart** to reboot the system.

This 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 System Setup > Server Settings > Redundant Configuration.
2. On the Redundant Configuration screen, click Switch Server Role.
   The system initiates a failover to the other server.

Discontinue a Redundant 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 205.
3. On the redundant server:
   a. Go to System Setup > Server Settings > Database.
   b. On the Database screen, deselect the Use an external SQL Server database check box.
   c. Click Update.
      The redundant server reboots.
4. On the primary server:
   a. Go to System Setup > Server Settings > Redundant Configuration.
   b. On the Redundant Configuration screen, click Reset Redundant Configuration.
      The primary system reboots.

When the system reboots, you can no longer access the system via the virtual IP. The redundant server is now a stand-alone system with an internal database, and the primary server is a stand-alone system with an external database.

To return to a redundant configuration, see “Implement a Redundant Polycom CMA 5000 System” on page 203
Add Your Own Logo to the Polycom CMA System User Interface

You can add your company logo on the Polycom CMA system user interface. To avoid distortion, we recommend adding a logo in GIF, JPG, or PNG format with a size no greater than 300 x 44 pixels.

To add your company logo to the Polycom CMA system user interface
1 Go to System Setup > Server Settings > Custom Logos.
2 In the Current Server Logo section of the Custom Logos screen, 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.

Add Your Own Logo to the Polycom CMA Desktop User Interface

You can add a custom 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 branded 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 your company logo Polycom CMA Desktop user interface**

1. Go to **System Setup > Server Settings > Custom Logos**.
2. In the **Current CMA Desktop Logo** section of the **Custom Logos** screen, 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.
Gatekeeper Management Operations

This chapter describes how to work with gatekeepers within the Polycom® Converged Management Application™ (CMA™) system. It includes these topics:

- Primary Gatekeeper Management Operations
- Add an Alternate Gatekeeper
- Edit the Alternate Gatekeeper Settings

Primary Gatekeeper Management Operations

By default the Polycom CMA system is made the primary gatekeeper during the First Time Setup process.

Edit the Primary Gatekeeper Settings

To edit the primary Polycom CMA system gatekeeper settings

1. Go to System Setup > Gatekeeper Settings > Primary Gatekeeper.
2. On the Primary Gatekeeper screen, make the required changes.
3. Click Update.
Alternate Gatekeeper Management Operations

Add an Alternate Gatekeeper

To add an alternate gatekeeper
1. Go to System Setup > Gatekeeper Settings > Alternate Gatekeeper.
2. On the Alternate Gatekeeper screen, enter the required gatekeeper information.
3. Click Update.

Edit the Alternate Gatekeeper Settings

To edit the alternate gatekeeper settings
1. Go to System Setup > Gatekeeper Settings > Alternate Gatekeeper.
2. On the Alternate Gatekeeper screen, make the required changes.
3. Click Update.

Remove the Alternate Gatekeeper

To remove the alternate gatekeeper settings
1. Go to System Setup > Gatekeeper Settings > Alternate Gatekeeper.
2. On the Alternate Gatekeeper screen, clear the Need to Register checkbox.
3. Click Update.
Neighboring Gatekeeper Management Operations

Add a Neighboring Gatekeeper

To add a neighboring gatekeeper
2. On the Neighboring Gatekeeper screen, click Add Neighbor.
3. In the Add Neighbor dialog box, enter the required gatekeeper information and click Update.

Edit a Neighboring Gatekeeper

To edit the settings for a neighboring gatekeeper
2. On the Neighboring Gatekeeper screen, 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
2. On the Neighboring Gatekeeper screen, select the neighboring gatekeeper of interest and click Delete.
3. Click Delete to confirm the deletion.
Management & Security Operations

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

- Edit Security Settings to Implement HTTPS
- Automatic Endpoint Discovery
- Set Common Passwords for Endpoints
- Update the Polycom CMA Server Software

Edit Security Settings to Implement HTTPS

By default, the Polycom CMA system uses standard http for its data interchanges. Edit the Security 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:

<table>
<thead>
<tr>
<th>Decision...</th>
<th>If yes, then perform these tasks...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the Polycom CMA system default key and certificate?</td>
<td>“Edit Security Settings to Implement HTTPS” on page 211</td>
</tr>
<tr>
<td>Use your own existing private key and certificate, if your company is self-authorizing?</td>
<td>“Upload a Private Key” on page 213, “Upload a Certificate” on page 213, “Edit Security Settings to Implement HTTPS” on page 211</td>
</tr>
<tr>
<td>Use a private key and certificate requested by the Polycom CMA system?</td>
<td>“Generate a Certificate Request” on page 212, “Upload a Certificate” on page 213, “Edit Security Settings to Implement HTTPS” on page 211</td>
</tr>
</tbody>
</table>
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.

**Table 23-1 Fields in the Certificate Request Data dialog box Fields for Certificate Request**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name</td>
<td>Two-letter (ASCII onlya) ISO 3166 country code</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>Full name (ASCII onlya)</td>
</tr>
<tr>
<td>Locality Name</td>
<td>City (ASCII onlya)</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Company Who (ASCII onlya)</td>
</tr>
<tr>
<td>Organization Unit Name</td>
<td>Section (ASCII onlya)</td>
</tr>
<tr>
<td>Common Name</td>
<td>Server’s host name (ASCII onlya)</td>
</tr>
<tr>
<td>Email Address</td>
<td>(ASCII onlya)</td>
</tr>
</tbody>
</table>

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.

**Generate a Certificate Request**

**To generate a certificate request on a PolycomCMA system**

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. See Table 23-1.
5 Save the Certificate Request Data to a file and submit the file to the Certificate Authority of your choice.

### Upload a Private Key

**To upload a private key to a Polycom CMA system**

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

**To upload a certificate from a Certificate Authority**

1. If necessary, save the certificate file to a PC on the network.
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
2. On the Security Settings screen, 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
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 certificate 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. When the HTTPS Security Alert appears, 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: se200” and asking you “Do you want to install this certificate?”
   g. 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.”

### Automatic Endpoint Discovery

After first-time setup, you can configure the Polycom CMA system to discover and configure any endpoints that register automatically with Polycom CMA system through the gatekeeper or Global Directory Server.

If automatic discovery and configuration is not successful, you can manually add endpoints.

#### Note

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. In addition, the Polycom CMA system only supports automatic discovery for V-Series, VSX-Series, and Polycom HDX-Series devices.

#### To enable automatic discover of endpoints


2. In the Automatic Endpoint Discovery section of the Device Management Settings screen, 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

2 In the Common Password section of the Device Management Settings screen, 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.

4 In a redundant configuration, repeat steps 1 through 3 on the redundant server.

**Update the Polycom CMA Server Software**

Refer to the *Polycom CMA Upgrade Guide* for information on upgrading your Polycom CMA software.
Dial Plan Setup Operations

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 and Site Link Operations
- Site Link Operations
- Gatekeeper Operations
- Dial Plan Service Operations
- Dial Rule Operations
- Least-Cost Routing Operations

Site and Site Link Operations

View the Graphical Site Topology

To view the graphical site topology

>> Go to System Setup > Dial Plan and Sites > Site Topology.

The Site Topology 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 System Setup > Dial Plan and Sites > Sites.

The Sites list appears. It includes this information:

Table 24-1  Information in the Sites List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The physical location of the site</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the site</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code for the site</td>
</tr>
<tr>
<td>Area Code</td>
<td>The area code for the site</td>
</tr>
</tbody>
</table>

Add a Site

To add a site

1  Go to System Setup > Dial Plan and Sites > Sites.
2  From 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. See Table 24-1.
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.
### Table 24-2 Site Provisioning Details fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date and Time Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>Specifies the country code for their location</td>
</tr>
<tr>
<td>Language</td>
<td>Specifies the display language for their user interface</td>
</tr>
<tr>
<td>Date Format</td>
<td>Specifies the date display format</td>
</tr>
<tr>
<td>Auto Adjust for Daylight Saving Time</td>
<td>Specifies whether or not to adjust the endpoint's system clock for daylight savings time</td>
</tr>
<tr>
<td>Time Format</td>
<td>Specifies the time display format</td>
</tr>
<tr>
<td>Time Server</td>
<td>Specifies whether to connect to a time server for automatic system time settings. If <strong>Time Server</strong> is set to <strong>Manual</strong> or <strong>Auto</strong> but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.</td>
</tr>
<tr>
<td>Time Server Address</td>
<td>Specifies the address of the time server when <strong>Time Server</strong> is set to <strong>Manual</strong></td>
</tr>
<tr>
<td>Timezone</td>
<td>Specifies the time difference between GMT (Greenwich Mean Time) and the endpoint system's location</td>
</tr>
<tr>
<td><strong>Firewall Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Use Fixed Ports</td>
<td>Specifies whether to define the TCP and UDP ports.</td>
</tr>
<tr>
<td>• If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>You must open the corresponding ports in the firewall. You must also open the firewall’s TCP port 1720 to allow H.323 traffic.</td>
</tr>
<tr>
<td>Start TCP Port</td>
<td>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 specify.</td>
</tr>
<tr>
<td>Note</td>
<td>You must also open the firewall’s TCP port 1720 to allow H.323 traffic.</td>
</tr>
<tr>
<td>Start UDP Port</td>
<td>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 specify.</td>
</tr>
</tbody>
</table>
### Table 24-2  Site Provisioning Details fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned…</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.460 Firewall Traversal</td>
<td>Allows the endpoint system to use H.460-based firewall traversal. For more information, see the Administrator’s Guide for Polycom HDX Systems.</td>
</tr>
</tbody>
</table>
| 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. |
| **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. |
| **LDAP Settings**      |                                                          |
| Enable LDAP Global Directory | Specifies whether to enable an (LDAP) enterprise directory |
| LDAP Default Group     | Specifies a default (LDAP) enterprise group for the endpoints systems. Set to **All** or to a specific enterprise group. |
| **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. When the value of this interval is set to 0, the endpoint systems do not poll the Polycom CMA system for new provisioning information. |
### Table 24-2  Site Provisioning Details fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Softupdate Polling Interval (minutes)</td>
<td>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. 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.</td>
</tr>
<tr>
<td>Quality of Service Settings</td>
<td></td>
</tr>
<tr>
<td>Video Type of Service Value</td>
<td>Specifies the IP Precedence or Diffserv value for video packets</td>
</tr>
<tr>
<td>Audio Type of Service Value</td>
<td>Specifies the IP Precedence or Diffserv value for audio packets</td>
</tr>
<tr>
<td>FECC Type of Service Value</td>
<td>Specifies the IP Precedence or Diffserv value for Far End Camera Control packets</td>
</tr>
<tr>
<td>Type of Service Field</td>
<td>Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Precedence</strong> — Represents the priority of IP packets sent to the system. The value can be between 0 and 5.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DiffServ</strong> — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.</td>
</tr>
<tr>
<td>Maximum Transmission Unit Size (bytes)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable PVEC</td>
<td>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</td>
</tr>
<tr>
<td>Enable RSVP</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Dynamic Bandwidth</td>
<td>Specifies whether to let the endpoint system automatically find the optimum line speed for a call.</td>
</tr>
<tr>
<td>Maximum Transmit Bandwidth (Kbps)</td>
<td>Specifies the maximum transmission line speed between 64 kbps and 4096 kbps.</td>
</tr>
<tr>
<td>Maximum Receive Bandwidth (Kbps)</td>
<td>Specifies the maximum reception line speed between 64 kbps and 4096 kbps.</td>
</tr>
<tr>
<td>Security Settings</td>
<td></td>
</tr>
<tr>
<td>Use Room Password for Remote Access</td>
<td>For room endpoint systems, specifies whether the room password and remote access password are the same.</td>
</tr>
<tr>
<td>Field</td>
<td>For the endpoint systems at the site being provisioned...</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Room Password</td>
<td>For room endpoint systems, enter or change the room password here. When the room password is set, you must enter it to configure the system Admin Settings using the remote control. The room password must not contain spaces.</td>
</tr>
<tr>
<td>Remote Access Password</td>
<td>For room 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.</td>
</tr>
<tr>
<td>Meeting Password</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Secure Mode</td>
<td>Specifies whether to operate in secure mode, which requires TLS, HTTPS, AES, digital signatures, and other security protocols, algorithms, and mechanisms. These protocols encrypt management communication over IP, preventing access by unauthorized users.</td>
</tr>
<tr>
<td>Enable Encryption</td>
<td>Specifies how to encrypt calls with other sites that support AES encryption.                                                                                                           • When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don’t support it.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Enable Web Access</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Telnet Access</td>
<td>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.</td>
</tr>
<tr>
<td>Enable SNMP Access</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 24-2  Site Provisioning Details fields

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
</table>
| 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 | For room endpoint systems, 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. |

### SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Specifies whether to enable SIP calls</th>
</tr>
</thead>
</table>
| Enable SIP        | Specifies the DNS name or IP address of the SIP Proxy Server. If you leave this field blank, no proxy server is used.  
  By default, the SIP signaling is sent to port 5060 on the proxy server. To specify a different port, add it to the address as shown here: 10.11.12.13:5070 |
| Proxy Server      | Indicating the protocol the endpoint system uses for SIP signaling. The SIP network infrastructure determines which protocol is required.  
  • **Auto** enables an automatic negotiation of protocols in the following order: TLS, TCP, UDP. This is the recommended setting for most environments.  
  • **TLS** provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS.  
  • **TCP** provides reliable transport via TCP for SIP signaling.  
  • **UDP** provides best-effort transport via UDP for SIP signaling. |

### System Settings

| Field                         | 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 Access to User Setup    | Specifies whether endpoint system users can save changes they make to the directory  
  | Allow Directory Changes      | Specifies whether to set the endpoint system to answer incoming point-to-point calls automatically  
  | Auto Answer Point-to-Point Calls | Specifies whether to set the endpoint system to answer incoming multipoint calls automatically   |
  | Auto Answer Multipoint Calls |                                                                 |

Polycom, Inc.
**Table 24-2  Site Provisioning Details fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>For the endpoint systems at the site being provisioned...</th>
</tr>
</thead>
</table>
| 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         | Enter the maximum number of minutes allowed for calls on the endpoint systems. When this time has expired, endpoint system users see a message asking them if they want to hang up or stay in the call. If they do not answer within one minute, the call automatically disconnects. If they choose to stay in the call at this time, they will not be prompted again.  
Set this value to 0 to remove any limit. |
| (minutes)                    |                                                                                                                                                                                                                                                                           |
| Recent Calls                 | Specifies whether to display the Recent Calls button on the endpoint system's 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 endpoint systems should remain awake during periods of inactivity. The default is 3 minutes. Setting this option to Off prevents the system from going to sleep.                                                                                                     |
| Address Displayed in         | Specifies whether to display the endpoint systems’ public or private address in the Global Address Book.                                                                                                                                                                      |
| Global Directory             |                                                                                                                                                                                                                                                                           |
| Presence Settings            |                                                                                                                                                                                                                                                                           |
| Enable Presence Directory    | Specifies whether to enable presence for endpoint systems at the site. If presence is enabled, the endpoints systems connect to the Polycom CMA system presence service.                                                                                                                                 |
| Service                      |                                                                                                                                                                                                                                                                           |
| CMA Desktop Settings         |                                                                                                                                                                                                                                                                           |
| Heartbeat Posting Interval   | Specifies the frequency at which the endpoint systems poll the Polycom CMA system for a heartbeat.                                                                                                                                                                         |
| (minutes)                    |                                                                                                                                                                                                                                                                           |
| In Call Stats Posting Interval (minutes) | Specifies the frequency at which the endpoint systems poll the Polycom CMA system for in call statistics |

---

226  Polycom, Inc.
# 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 **System Setup > Dial Plan and Sites > Sites**.
2. From 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. See Table 24-1.
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 **System Setup > Dial Plan and Sites > Sites** or **System Setup > Dial Plan and Sites > Site Topology**.
2. From 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.

### Table 24-3  Fields on the Link Editor Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Name</td>
<td>Name (ASCII onlya) of the inter-site link</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII onlya) of the inter-site link</td>
</tr>
<tr>
<td>From Site</td>
<td>Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet.</td>
</tr>
<tr>
<td>To Site</td>
<td>Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet or VPN option.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Specifies a direct link between two physical sites or a multisite link, for which a path of links is defined</td>
</tr>
<tr>
<td>Bandwidth (Kbps)</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Bit Rate (Kbps)</td>
<td>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.</td>
</tr>
</tbody>
</table>

a. For more information, see “Field Input Requirements” on page 6.
View the Site Links List

Table 24-4  Information in the Site Links List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the link</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the link</td>
</tr>
<tr>
<td>From Site</td>
<td>First site reached in the call route</td>
</tr>
<tr>
<td>To Site</td>
<td>Final site reached through this call link</td>
</tr>
<tr>
<td>Link Type</td>
<td>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</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>The maximum bandwidth (Mbps) for video available on this link (for direct links only)</td>
</tr>
</tbody>
</table>

To view the Site Links list

>> Go to System Setup > Dial Plan and Sites > Site-Links.

The Site-Links list appears.

Table 24-5  Information in the List of Inter-site Links Screen

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Name</td>
<td>Name of the link</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the link</td>
</tr>
<tr>
<td>From Site</td>
<td>First site reached in the call route</td>
</tr>
<tr>
<td>To Site</td>
<td>Final site reached through this call link</td>
</tr>
<tr>
<td>Link Type</td>
<td>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</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>The maximum bandwidth (Mbps) for video available on this link (for direct links only)</td>
</tr>
</tbody>
</table>
Add a Site Link

To add a site link

1. Go to System Setup > Dial Plan and Sites > Site-Links.
2. From 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. See Table 24-5.
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.
   d. Add additional site links as required.
   e. Click Save.

The new link appears on the List of site Links screen.

Note
If you receive a Select Destination Place dialog box, click OK and continue.

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 System Setup > Dial Plan and Sites > Site-Links.
2. From 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. See Table 24-5.
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 System Setup > Dial Plan and Sites > Site-Links.
2. From the Site-Links list, select the site link of interest and click Delete Site-Link.
3. Click Yes to confirm the deletion.

Gatekeeper Operations

A gatekeeper region is a group of sites that share a common Polycom CMA system and gatekeeper. When you first set up the Polycom CMA system, a default region and a default site exist, and the default site is automatically associated with the default gatekeeper region. You may change the name of the default gatekeeper region 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.
To view the neighboring gatekeepers

Go to System Setup > Gatekeeper Settings > Neighboring Gatekeepers.

The Neighboring Gatekeepers list appears.

Table 24-7  Information in the Neighboring Gatekeepers List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the region</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the region</td>
</tr>
</tbody>
</table>

Add a Neighboring Gatekeeper

To enable a gatekeeper-to-gatekeeper relationship, create a neighboring gatekeeper.

To add a neighboring gatekeeper

1 Go to System Setup > Gatekeeper Settings > Neighboring Gatekeepers.
2 From the Neighboring Gatekeepers screen, click Add Neighbor.
3 In the **Add Neighbor** dialog box, enter a **Name** and **Description** and other required information. See Table 24-6.
4 Click **Save**.
   The neighboring gatekeeper is added to the system.

**Edit a Neighboring Gatekeeper**

To **edit a neighboring gatekeeper**
1 Go to **System Setup > Gatekeeper Settings > Neighboring Gatekeepers**.
2 From the **Neighboring Gatekeepers** screen, click **Edit Neighbor**.
3 In the **Edit Neighbor** dialog box, edit the information as required. See Table 24-6.
4 Click **Save**.

**Delete a Neighboring Gatekeeper**

You can delete a gatekeeper-to-gatekeeper relationship from the Polycom CMA system.

**Note**
Routing between gatekeepers works only when both regions are defined in the Polycom CMA system.

To **delete a neighboring gatekeeper**
1 Go to **System Setup > Gatekeeper Settings > Neighboring Gatekeepers**.
2 From the **Neighboring Gatekeepers** screen, select the region of interest and click **Delete Neighbor**.
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.

For details on how the Conference on Demand service is configured, see Table 24-8.

**Table 24-8  Conference on Demand Service Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info Tab</strong></td>
<td></td>
</tr>
<tr>
<td>Service Type</td>
<td>Conference on Demand (read only)</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates whether or not the service is enabled</td>
</tr>
<tr>
<td>Available for New Groups</td>
<td>Indicates whether or not the service is available for new user groups</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII only) of the service. By default for this service, Conference on Demand</td>
</tr>
<tr>
<td>Service Prefix</td>
<td>The prefix (ASCII only) for the service. By default for this service: con</td>
</tr>
<tr>
<td><strong>Conference on Demand tab--MCU Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Login ID</td>
<td>User login (ASCII only) for the MCU hosting the conference. This user account must be authorized to create new conferences.</td>
</tr>
<tr>
<td>Password</td>
<td>Password (ASCII only) for the user login. Each time you modify the password for the MCU, you must also modify it in this screen.</td>
</tr>
</tbody>
</table>
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. For details, see Table 24-9.

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 screen.
- Gateway services must be defined.
- The LCR table must be defined.

### Table 24-8 Conference on Demand Service Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 Network Service</td>
<td>The corresponding service created on the MCU to implement this Polycom CMA system service. Set on the MCU (ASCII only)</td>
</tr>
</tbody>
</table>

**Default Conference Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGC: Video Session</td>
<td>Indicates what users see. Set to Continuous Presence for this service.</td>
</tr>
<tr>
<td>Notes</td>
<td>• MGC only. For the RMX 2000 MCU, the profile determines this setting.</td>
</tr>
<tr>
<td></td>
<td>• Select Transcoding to support IP and ISDN calls.</td>
</tr>
<tr>
<td>MGC: Bit rate (Kbps)</td>
<td>Default bit rate for calls.</td>
</tr>
<tr>
<td>Notes</td>
<td>• MGC only. The RMX 2000 MCU bit rate is dictated by the RMX profile.</td>
</tr>
<tr>
<td></td>
<td>• The video endpoint system that starts the Conference on Demand call may use a higher or lower bit rate than is specified in this screen.</td>
</tr>
<tr>
<td>RMX: Profile Name</td>
<td>The name of the RMX profile that has the conference settings for the conference.</td>
</tr>
</tbody>
</table>

Notes:
- 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. For details, see Table 24-9.

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 screen.
- Gateway services must be defined.
- The LCR table must be defined.
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 screen.

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 screen does not include gateway services, alternate routing and least-cost routing are disabled. For details, see the following table.

Table 24-10 Fields in the Gateway Service dialog box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Name of the service (read only)</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates whether this service is enabled</td>
</tr>
<tr>
<td>Available for New Groups</td>
<td>The service is available for new user groups</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the service</td>
</tr>
<tr>
<td>Service Prefix</td>
<td>The prefix for this service: 9.</td>
</tr>
</tbody>
</table>

Table 24-9 Fields in the Simplified Dialing Service dialog box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Name of the service (read only)</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates whether this service is enabled</td>
</tr>
<tr>
<td>Available for New Groups</td>
<td>The service is available for new user groups</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the service</td>
</tr>
<tr>
<td>Service Prefix</td>
<td>The prefix for this service: 9.</td>
</tr>
</tbody>
</table>
Table 24-10 Fields in the Gateway Service dialog box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Prefix</td>
<td>The prefix for this service. Must be a registered E.164 alias for the corresponding gateway in the Devices screen for Directory Setup.</td>
</tr>
<tr>
<td>For use in simplified dialing</td>
<td></td>
</tr>
<tr>
<td>Device Capability</td>
<td>Specifies the type of connection the device can handle. Select all that apply. Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>H.320.</strong> Supports video and voice using the ITU H.320 standard.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Voice.</strong> Supports voice over the PSTN network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other.</strong> Supports a protocol other than H.320 or voice, such as H.321 or video over ATM.</td>
</tr>
<tr>
<td>Bit Rate (Kbps)</td>
<td>The maximum rate at which the calls can connect.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you select <strong>Unknown</strong>, this service cannot support simplified dialing.</td>
</tr>
<tr>
<td>Insert between prefix and first number</td>
<td>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</td>
</tr>
<tr>
<td>Insert between phone number</td>
<td>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</td>
</tr>
<tr>
<td>Append after full dial string</td>
<td>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**</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> 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<strong>3452</strong></td>
</tr>
</tbody>
</table>
**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 screen 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. For details, see Table 24-11.

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.

**Table 24-11 Fields in the MCU Service dialog box**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Enable</td>
<td>Indicates whether this service is enabled or not.</td>
</tr>
<tr>
<td>Available for New Groups</td>
<td>The service is available for new user groups.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the service. To identify it easily in the List of Services screen, include the prefix and the MCU feature (for example, 384 K video switching).</td>
</tr>
<tr>
<td>Service Prefix</td>
<td>The prefix for this service, which must be a E.164 alias that is registered for the MCU on the Device screen.</td>
</tr>
</tbody>
</table>

**View the Services List**

This screen shows the services that have been defined in your dial plan. These services are available when you place unscheduled calls. For details, see Table 24-12.

**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 System Setup > Dial Plan > Services.

The Services list appears.

Table 24-12 Information in the Services List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Prefix of the service.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of service. Available types include System, Gateway, and MCU.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the service.      Tip: When completed automatically, the description reflects the value entered in the MGC or RMX 2000 manager.</td>
</tr>
<tr>
<td>Enabled</td>
<td>By default, services are enabled. To disable them, clear the Enabled check box.</td>
</tr>
</tbody>
</table>

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 System Setup > Dial Plan > Services.
2. From 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. See Table 24-8.
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 System Setup > Dial Plan > Services.
2. From 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. See Table 24-8.
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 System Setup > Dial Plan > Services.
2. From 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.
Table 24-13  Fields on the Dial Rule Editor: General Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Info</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name (ASCII only) of the dial rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Description (ASCII only) of the dial rule, which can be up to 256 characters long.</td>
</tr>
<tr>
<td>Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Select the check box to enable the rule.</td>
</tr>
<tr>
<td>Pattern Type</td>
<td>Specifies the type of pattern to be matched. Available patterns include:</td>
</tr>
<tr>
<td></td>
<td>• Local Directory Services</td>
</tr>
<tr>
<td></td>
<td>• DNS Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Prefix</td>
</tr>
<tr>
<td></td>
<td>• Prefix Range</td>
</tr>
<tr>
<td>Applicable Site</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Routing Action &gt; Dial String Manipulation</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address Pattern Data</td>
<td>Specifies the criteria (ASCII only) to use to match the pattern type and additional changes to make when routing the call.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Start Value</td>
<td>The starting number to use as a prefix, which displays only for rules with the Prefix Range pattern type.</td>
</tr>
<tr>
<td>End Value</td>
<td>The ending number to use as a prefix, which displays only for rules with the Prefix Range pattern type.</td>
</tr>
<tr>
<td># Characters to remove</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 24-13 Fields on the Dial Rule Editor: General Screen (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |

### 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. Table 24-14 shows the available pattern types.

**Table 24-14 Available Pattern Types**

<table>
<thead>
<tr>
<th>Pattern Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Directory</td>
<td>Search the List of Devices and List of Services. Includes aliases, which are</td>
</tr>
<tr>
<td>Services</td>
<td>searched before the service prefix.</td>
</tr>
<tr>
<td>DNS Name</td>
<td>Look up a DNS Name</td>
</tr>
<tr>
<td>IP Address</td>
<td>Look for an IP addresses in the IPV4 format</td>
</tr>
<tr>
<td>Prefix</td>
<td>Look for a prefix specified in the dial rule</td>
</tr>
<tr>
<td>Prefix Range</td>
<td>Look for a prefix within the range of prefixes specified in the dial rule</td>
</tr>
</tbody>
</table>
### Routing Actions

A routing action informs the Polycom CMA system what to do based on the dial rule’s associated pattern type. Table 24-15 shows the available routing actions.

#### Table 24-15  Available Routing Actions

<table>
<thead>
<tr>
<th>Routing Action</th>
<th>Pattern Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route</td>
<td>All</td>
<td>Allow the call to pass</td>
</tr>
<tr>
<td>Block</td>
<td>All</td>
<td>Block the call</td>
</tr>
<tr>
<td>Route within region</td>
<td>IP Address</td>
<td>Route to any IP address inside the region</td>
</tr>
<tr>
<td>Route out of region</td>
<td>IP Address</td>
<td>Route to any IP address outside the region</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>The originating site's Internet access rules still apply.</td>
</tr>
<tr>
<td>Route to a gateway with LCR</td>
<td>Prefix and Prefix Range</td>
<td>Remove the prefix specified in the dial rule and route the remaining dial string to a gateway service, which has the specified LCR table</td>
</tr>
<tr>
<td>Route to a gateway service</td>
<td>Prefix and Prefix Range</td>
<td>Remove the prefix specified in the dial rule and route the remaining dial string to the specified gateway service</td>
</tr>
<tr>
<td>Route to a list of gateway services</td>
<td>Prefix and Prefix Range</td>
<td>Modify the dial string specified in the dial rule and route the remaining dial string to the specified gateway service.</td>
</tr>
<tr>
<td>Route to a trusted neighbor</td>
<td>Prefix and Prefix Range</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>The neighboring gatekeeper must be configured as a region in the CMA system.</td>
</tr>
</tbody>
</table>
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 screen, 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.

View the Dial Rules List

To view the Dial Rules list

>> Go to System Setup > Dial Plan > Dial Rules.

The Dial Rules list appears.

<p>| Table 24-16  Information in the List of Dial Rules Screen |</p>
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the dial rule</td>
</tr>
<tr>
<td>Pattern Type</td>
<td>The pattern type in use for this rule. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Local Directory Services</td>
</tr>
<tr>
<td></td>
<td>• DNS Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• Prefix</td>
</tr>
<tr>
<td></td>
<td>• Prefix Range</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Parts of a Dial Rule” on page 243.</td>
</tr>
<tr>
<td>Pattern Data</td>
<td>Additional criteria that must be met to apply this rule</td>
</tr>
</tbody>
</table>
Add a Dial Rule

Table 24-16  Information in the List of Dial Rules Screen (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Action</td>
<td>The routing action used by this rule. Options are:</td>
</tr>
<tr>
<td></td>
<td>• Route</td>
</tr>
<tr>
<td></td>
<td>• Block</td>
</tr>
<tr>
<td></td>
<td>• Route within region</td>
</tr>
<tr>
<td></td>
<td>• Route out of region</td>
</tr>
<tr>
<td></td>
<td>• Route to a GW with LCR applied</td>
</tr>
<tr>
<td></td>
<td>• Route to a GW service</td>
</tr>
<tr>
<td></td>
<td>• Route to a list of GW services</td>
</tr>
<tr>
<td></td>
<td>• Route to a trusted neighbor</td>
</tr>
<tr>
<td>Note</td>
<td>Not all actions are available for all pattern types.</td>
</tr>
<tr>
<td>Site</td>
<td>The sites for which this rule is used. May be all sites or a specific site</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority assigned this rule</td>
</tr>
<tr>
<td>Enabled</td>
<td>Indicates whether or not the dial rule is enabled</td>
</tr>
</tbody>
</table>

Add a Dial Rule

To add a dial rule

2. From 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. See Table 24-8.
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**
2. From the Dial Rules list, select the dial rule of interest and click Edit Dialing Rule.
3. On the Dial Rules - General Information screen, check or uncheck the Enabled check box.
4. Click OK.

Edit a Dial Rule

**To edit a dial rule**
2. From 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.

**Table 24-17  Example of Least-Cost Routing Table**

<table>
<thead>
<tr>
<th>Country Code</th>
<th>Area Code</th>
<th>Prefix</th>
<th>Weighted Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>408</td>
<td>565</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>408</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>650</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>415</td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>
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.

**Table 24-18 LCR for Site A**

<table>
<thead>
<tr>
<th>Area Code</th>
<th>Prefix</th>
<th>Weighted Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>408</td>
<td>755</td>
<td>0</td>
</tr>
<tr>
<td>408</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>650</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>510</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>925</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>415</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>831</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>213</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>310</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>714</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>
The following table lists area codes for Washington, D.C., Eastern Maryland, and Northeastern Virginia.

Table 24-19  LCR for Site C

<table>
<thead>
<tr>
<th>Area Code</th>
<th>Prefix</th>
<th>Weighted Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>202</td>
<td>238</td>
<td>0</td>
</tr>
<tr>
<td>202</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>240</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>301</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>741</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>703</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>410</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>443</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>540</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>804</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>

The following table lists area codes for San Jose, Monterrey, and Southern California.

Table 24-20  LCR for Site B

<table>
<thead>
<tr>
<th>Area Code</th>
<th>Prefix</th>
<th>Weighted Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>831</td>
<td>477</td>
<td>0</td>
</tr>
<tr>
<td>831</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>408</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>213</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>310</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>714</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>
**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

Table 24-21  Fields of the LCR Tables List

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name (ASCII only) for the LCR table.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) (ASCII only)</td>
</tr>
<tr>
<td>Country</td>
<td>Country code for the location to which this call is made.</td>
</tr>
<tr>
<td>City Code</td>
<td>City or area code for the location to which this call is made.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The prefix is the first three numbers in a 7-digit dial string.</td>
</tr>
<tr>
<td># Digits to Strip</td>
<td>The number of digits to strip before dialing.</td>
</tr>
<tr>
<td>Cost</td>
<td>Weighted cost for each call to the selected area or city code.</td>
</tr>
</tbody>
</table>

Table 24-22  Information in the LCR Tables List

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the LCR table.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the LCR table.</td>
</tr>
</tbody>
</table>

View the Least Cost Routing Tables List

To display the list of least cost routing tables

Go to System Setup > Dial Plan > LCR Tables.

The LCR Tables list appears.
Add a Least Cost Routing Table

To add a LCR table
1. Go to System Setup > Dial Plan > LCR Tables.
2. From 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. See Table 24-21.
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 System Setup > Dial Plan > LCR Tables.
2. From 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. See Table 24-21.
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 System Setup > Dial Plan > LCR Tables.
2. From the LCR Tables list, select the table of interest and click Delete LCR.
3. Click Delete to confirm the deletion.
**ACF (Admission Confirm)**
A message sent by the gatekeeper to the calling endpoint that the ARQ was accepted.

**Address Resolution**
A process that identifies the IP address of the called endpoint when the calling endpoint uses an H.323 alias to dial.

**Administrator**
A role that grants permissions to access all capabilities throughout CMA, including access to the Administrator View, Operator View, and My Conferences View.

**Alias**
Character or numerical string used to identify an endpoint. Is resolvable to an IP address of a device. E.164 and H.323 ID are frequently used aliases.

**Alternate Gatekeeper**
A gatekeeper that devices can use when their primary gatekeeper is unreachable.

**Alternate Routing**
A method of routing a call through an alternate protocol (for example, H.320), when the call cannot proceed through the original route at an acceptable bandwidth.

**ARJ (Admission Reject)**
A message sent by the gatekeeper to the calling endpoint that the ARQ was rejected.

**ARQ (Admission Request)**
A message sent to the gatekeeper by the calling or receiving endpoint requesting that a call take place.
**Bandwidth**
The amount of information that can be sent over a given transmission channel, usually expressed as bits per second.

**BCF (Bandwidth Confirm)**
A message sent by the gatekeeper to the calling endpoint that the bandwidth request (BRQ) was accepted.

**Bit Rate**
The number of bits occurring per unit time, usually expressed as bits per second.

**BRI (Basic Rate Interface)**
BRI is the standard copper line ISDN service, and usually consists of two 64 Kbs channels and one 16 Kbs signalling channel.

**BRJ (Bandwidth Reject)**
A message sent by the gatekeeper to the calling endpoint that the bandwidth request (BRQ) was rejected.

**BRQ (Bandwidth Request)**
A message sent to the gatekeeper from the endpoint requesting a change to the allowed bandwidth when placing a call.

**Call Routing System**
Provides system services for Simplified Dialing and Conference on Demand through a specific prefix.

**Call Signaling Address**
The IP address and port used to communicate H.225 call control messages.

**Circuit-switched Networks**
ISDN, ATM, and leased lines.

**CLID (Calling Line Identifier)**
Also known as caller ID, in which the name and number of the calling party is sent to the receiving endpoint.

**Codec**
A device or software that converts analog pictures and voice into a compressed digital stream across the network between conferencing sites.
Continuous Presence
A video layout mode, during which several participants can be viewed simultaneously on the screen during a conference.

If the number of participants is less than or equal to the number of participants displayed, each participant can see all the other participants. If the number of participants exceeds the number of screens in the selected continuous presence layout, automatic video switching occurs.

DCF (Disengage Confirm)
A message sent by the gatekeeper to the calling endpoint that the request for call disengagement was accepted.

Dedicated Link
A service that provides a logical connection between two networks separated geographically, in which the allotted bandwidth is not shared.

Default Gatekeeper
The gatekeeper with which video endpoint systems register if they are set to auto-register, instead of entering the IP for a specific gatekeeper.

Device
A device indicate equipment that is on your video conferencing network. In CMA, devices include endpoints (sometimes called terminals), MCUs (multi-point control units), and gateways.

DHCP (Dynamic Host Configuration Protocol)
DHCP servers allow multiple devices to share a group of IP addresses, assigning one to a specific device, if needed.

Dial Plan
A collective term used to define all the settings related to video call routing, which includes the collection of sites, links, regions, dial rules, services, and least-cost routing tables.

Dial Plan Service
A service created through dial plan setup. Two default dial plan services are available: Conference on Demand and Simplified Dialing.

Dialing Rule
A dialing rule describes how CMA locates a specific endpoint and routes a call. A dialing rule consists of pattern types and routing actions.

Dial String
The string of numbers used to dial an endpoint.
**DID (Direct Inward Dial)**
Enables endpoints that do not have native ISDN to have a dedicated direct number.

**Direct Connection**
A physical connection between an MCU and an endpoint through a serial cable.

**Direct Links**
An inter-site link that goes directly between sites.

**DNS Name**
The name of a device on an IP network, as specified by a DNS (Domain Name System) server. Also called the host name.

**DRJ (Disengage Reject)**
A message sent by the gatekeeper to the calling endpoint that the request for call disengagement was rejected.

**DRQ (Disengage Request)**
A message sent by the gatekeeper to the calling endpoint that the request for call disengagement was accepted.

**E.164**
An H.323 alias that is resolvable by a gatekeeper. Functions as an extension. E.164 is the international public telecommunications numbering plan used for standard telephone numbers (that is, digits 0 through 9, * and #). In CMA, E.164 provides the extension or a telephony-based alias to reach an H.323 device.

**E-mail Address**
An H.323 alias that is resolvable by a gatekeeper. Usually appears in the form of alias@organization.com.

**Embedded MCU**
A video endpoint system that includes multi-point capability.

**Endpoint**
An H.323 entity that can call or be called. In the CMA system, called a device.

**Equipment**
Called a device in the CMA system.
**Gatekeeper**
An H.323 entity that provides address translation and controls access to the network for H.323 endpoints. May also provide services to endpoints.

**Gatekeeper Identifier**
The identifier of this gatekeeper on the network for communication between endpoints and CMA.

**Gateway**
An H.323 entity that provides real-time, two-way communication between terminals on a packet-based network and a switched-circuit network. Gateways allows devices on networks that use different protocols (such as ISDN and IP) to communicate with each other.

**Gateway Services**
Gateway services tell CMA how to route a call when converting between IP and ISDN by using a specified prefix.

**GCF (Gatekeeper Confirm)**
A message sent by the gatekeeper to the endpoint that the registration request was accepted.

**GRJ (Gatekeeper Reject)**
A message sent by the gatekeeper to the endpoint that the registration request was rejected.

**GRQ (Gatekeeper Request)**
A message sent to the gatekeeper by an endpoint requesting registration.

**H.225**
The signaling protocol for multimedia communications as defined in the ITU-T Recommendation. Consists of the RAS Channel (for gatekeeper-to-endpoint communications) and the Call Signaling Channel (to establish a call between two endpoints).

**H.245**
The control protocol for multimedia communications as defined in the ITU-T Recommendation. The control channel provides end-to-end control of a call between endpoints.

**H.320 ITU-T**
Standard that defines the protocols used for multimedia communications on switched networks, such as ISDN.
**H.323 ITU-T**
Standard that defines the protocols used for multimedia communications on packet-based networks, such as IP.

**H.323 ID**
An H.323 alias composed of alphanumeric characters.

**Inter-site Link**
A logical connection from one LAN to another LAN within the WAN or from one physical site to another physical site that is outside the enterprise.

**IP Address**
A unique identifier for a computer on a TCP/IP network.

**IRQ (Information Request)**
A RAS message sent to the gatekeeper by the calling or receiving endpoint requesting information.

**IRR (Information Response)**
A RAS message sent by the gatekeeper to the calling or receiving endpoint as a response to the IRQ.

**ISDN (Integrated Services Digital Network)**
A switched network service that provides end-to-end digital connectivity to transmit voice, data, and video simultaneously over a single line.

ISDN is the global standard for digital dial services. The network consists of a basic rate (two channels at 64 Kbit per second) and a primary rate (32 channels).

**IVR (Interactive Voice Response) Service**
A voice-response system that replies to a call and prompts the caller to provide additional information, such as an extension to dial or an entry passcode.

**Jitter**
The uneven arrival of data, resulting from a one-way packet delay of more than 150 milliseconds.

**LAN (Local Area Network)**
A data communications network that connects two or more data communication devices over a transmission medium.

**LCF (Location Confirm)**
A message sent by the gatekeeper, notifying the endpoint or gatekeeper that the location confirmation was accepted.
**LCR (Least-Cost Routing)**
The routing of IP calls through a call processing server, using the most cost-effective path.

**Least-Cost Routing Tables**
LCR tables illustrate the relative cost of using a particular gateway service from a specified site to a set of destination countries and cities. These tables are used to determine the least expensive route for a call.

**LDAP (Lightweight Directory Access Protocol)**
Light-weight directory access protocol. An Internet protocol that e-mail and other programs use to look up information on a server.

**Line Hunting**
The ability of a gatekeeper to find an available gateway for outbound calls, according to the RAI information.

**Link**
See *Inter-site Link*.

**Logical Bandwidth Controls**
The maximum bandwidth that is allowed for video communications over any link or pipe. This number is entered in CMA for each inter-site link.

**LRJ (Location Reject)**
A message sent by the gatekeeper to the endpoint or gatekeeper that the location confirmation was rejected.

**LRQ (Location Request)**
A message sent to the gatekeeper by an endpoint or another gatekeeper, requesting the location of an endpoint.

**LWRRQ (Lightweight Registration Request)**
A message sent to the gatekeeper by a registered endpoint, requesting to remain registered.

**MCU (Multipoint Control Unit)**
An H.323 endpoint that supports multipoint conferencing for three or more endpoints. Also called a device.

**MCU Service**
MCU services tell CMA how to route a call with a particular MCU feature by using a specific prefix.
Multipoint Conference
A conference that includes three or more terminals.

Multisite Link
An multisite link consists of two or more direct links.

Neighboring Gatekeepers
Gatekeepers that are configured in the neighboring gatekeeper table, enabling more efficient address resolution.

Network Address
A network number (such as 172.18.16.0) and a subnet mask (such as 255.255.248.0). These numbers are often represented by the following notation (172.18.16.0/255.255.248.0).

Operator
A role that grants permissions to access capabilities in the CMA Operator View.

Permissions
Access rights to use various CMA features. Permissions are granted through roles.

Party Number
A telephone number that may be from the originator or receiver.

Point-to-Point Call
A conference between two terminals.

POTS (Plain Old Telephone System)
The analog phone system (including telephones, modems, central offices switches, and so on) used around the world.

Proxy
A device that may be used to hide the true signaling address of an H.323 device from devices in other zones, while still allowing inter-zone calling.

QoS (Quality of Service)
Characterized by data rate and bit error rate. Good QoS indicates a high data rate that is uncompromised by low bit error rate. On packet-switched networks, QoS is not guaranteed.
RAI/RAC (Resource Availability Indicator/ Resource Availability Confirm)
RAI/RAC provides a mechanism that enables a gatekeeper to understand whether endpoints have available resources to take additional calls.

RAS (Registration Admission Status)
A protocol for registration, admission, and status, as defined in the H.225 Recommendation.

RAS Address
The IP address that includes the port for communicating registration, admission, and status messages.

RAS Channel
Channel that is used to show registration, admission, bandwidth change and status messages between two H.323 entities.

RCF (Registration Confirm)
A message sent by the gatekeeper to the endpoint that the registration request was accepted.

Region
A collection of sites managed by a single CMA server and gatekeeper.

Registrant
An endpoint that is an entry in the gatekeeper registry.

Routed Mode
The routing of a call that forms a direct connection between two endpoints through the gatekeeper.

RRJ (Registration Reject)
A message sent by the gatekeeper to the endpoint rejecting the registration request.

RRQ (Registration Request)
A message sent to the gatekeeper from an endpoint requesting registration.

SBC (Session Border Control)
A device that specifies call routing through the Internet for a site.

Scheduler
A role that assigns the permission to schedule conferences through CMA. Roles are assigned to users.
**Service**

See *Network Service* and *Dial Plan Service*.

**Site**

A site is a physical location within an enterprise. A site contains one or more LAN networks. A site may have multiple gateways to connect the IP network to the PSTN network. A site may also be the location of a specific endpoint. In CMA, a site is a physical area, such as a campus, in which many endpoints are located.

**Static Address**

An address that is manually entered into the address book. The address is considered static, because it is not updated when devices change.

**Subnet**

A part of a network that has been subdivided and controlled by a subnet mask. Network devices within a subnet have a similar IP addresses, defined with the base IP address and a bit mask.

**Subnet Mask**

The mask of an endpoint address that is matched to the network IP address.

**Switching (Video Switching)**

A video layout mode in which all participants see the same picture (video). The current speaker is displayed in full screen on all the participants’ endpoints, and the switching between participants is voice-activated. Whenever a participant speaks, this person becomes the conference speaker and is viewed on all screens.

**System**

Called a device in the CMA system.

**T.120**

ITU-approved standards for data conferencing that specify how documents should be moved, viewed, and changed in a conference.

**TCS4**

A method for dialing an endpoint using a gateway number and an extension.

**Terminal**

An H.323 endpoint that provides real-time, two-way communication with another H.323 endpoint. This communication format may be audio, video, or data.
Transcoding
A video session mode in which participants can use different line rates, video, audio, and data formats, while maintaining the highest video and audio capability each participant can achieve with an endpoint. The current speaker is displayed in full screen on all participants’ endpoints, and the switching between participants is voice-activated.

Transport Address
Consists of a network address and the TSAP Identifier of an addressable H.323 entity.

UCF (Unregister Confirm)
A message sent by the gatekeeper to the requesting endpoint that the unregistration request was accepted.

URJ (Unregister Reject)
A message sent by the gatekeeper to the requesting endpoint that the unregistration request was rejected.

URL (Universal Resource Locator)
The address of a computer or a file that is accessible through HTTP.

URQ (Unregistration Request)
A message sent by the endpoint requesting removal from the gatekeeper registry.

VoIP (Voice over IP)
Audio communications that use the IP communication network as the transmission medium.

Zone
A collection of endpoints (gateways, MCUs, and terminals) that a single gatekeeper manages. At a minimum, a zone must consist of one terminal and one gatekeeper.
This chapter has Polycom® Converged Management Application™ (CMA™) system troubleshooting information. It includes the following topics:

- Registration Problems and Solutions
- Point-to-Point Calling Problems and Solutions
- MCU and Gateway Dialing Problems and Solutions
- Conference On Demand Problems and Solutions

Note
Some recommended solutions require access to screens in the Administrator View. The default Scheduler or Operator permissions do not provide access to this view. You must log in as an administrator to access this view.

### Registration Problems and Solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to place calls to an MCU conference room from a registered Polycom HDX system</td>
<td>The Polycom CMA system rejects the ARQ stating that the &quot;endpoint is not registered&quot; to the gatekeeper even though the system indicates it is registered.</td>
<td>• The MCU is not registered to the gatekeeper</td>
</tr>
</tbody>
</table>
| 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 **System Setup > Gatekeeper Settings > Primary Gatekeeper** screen.  
  • 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. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>An endpoint cannot register with the Polycom CMA system.</td>
<td>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.</td>
<td>- 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.</td>
</tr>
<tr>
<td>An endpoint cannot register with the Polycom CMA system.</td>
<td>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.</td>
<td>- Verify that the IP address that the gatekeeper sent to the endpoint is correct.</td>
</tr>
<tr>
<td>The MCU cannot register with the Polycom CMA system.</td>
<td>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.</td>
<td>- Verify that the Default Gatekeeper check box is selected in the System Setup &gt; Gatekeeper Settings &gt; Primary Gatekeeper screen. - Reset the MCU or MGC card to force registration to occur.</td>
</tr>
<tr>
<td>An endpoint shows that it is not registered to the gatekeeper in the Gatekeeper Registration field in the Device Status.</td>
<td>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 System Setup &gt; Gatekeeper Settings &gt; Primary Gatekeeper screen.</td>
<td>- Reboot the endpoint.</td>
</tr>
<tr>
<td>The RadVision OnLAN MCU continually changes state: from online to offline and offline to online.</td>
<td>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 System Setup &gt; Gatekeeper Settings &gt; Primary Gatekeeper screen.</td>
<td>- 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.</td>
</tr>
<tr>
<td>Problem</td>
<td>Description</td>
<td>Solutions</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| 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 **System Setup > 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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewStation and ViaVideo have an incorrect RAS IP address.</td>
<td>These endpoints are configured with a NAT address and may not receive the RCF message from the gatekeeper.</td>
<td>The endpoints need to be reconfigured to disable NAT.</td>
</tr>
</tbody>
</table>
| 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 System Setup > 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 System Management > 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 System Setup > 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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call fails when using an MCU service. Dialing an MCU service results in a network error.</td>
<td>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.</td>
<td>• Check the <a href="#">System Management &gt; Reports &gt; Gatekeeper Message Log</a> 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 <a href="#">System Setup &gt; Dial Plan and Sites &gt; Services</a> screen. Verify that the MCU service prefix is enabled and listed.</td>
</tr>
<tr>
<td>Simplified dialing does not work. When you dial 9, you receive a network error.</td>
<td>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.</td>
<td>• Check the <a href="#">System Management &gt; Reports &gt; Gatekeeper Message Log</a> for error messages. • Verify that the gateway and simplified dialing service prefix is enabled. Go to <a href="#">System Setup &gt; Dial Plan and Sites &gt; Services</a>. • Verify that the gateway is registered.</td>
</tr>
</tbody>
</table>
Conference On Demand Problems and Solutions

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Solutions</th>
</tr>
</thead>
</table>
| 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 System Setup > Dial Plan and Sites > Services. |

Gatekeeper Cause Codes

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>The gatekeeper is out of resources</td>
</tr>
<tr>
<td>151</td>
<td>The gatekeeper has insufficient resources</td>
</tr>
<tr>
<td>152</td>
<td>The gatekeeper registration version is invalid</td>
</tr>
<tr>
<td>153</td>
<td>The call signal address is invalid</td>
</tr>
<tr>
<td>154</td>
<td>The registering device’s address is invalid</td>
</tr>
<tr>
<td>155</td>
<td>The registering device’s terminal type is invalid</td>
</tr>
<tr>
<td>156</td>
<td>The registering device’s permissions are invalid</td>
</tr>
<tr>
<td>157</td>
<td>The conference ID is invalid</td>
</tr>
<tr>
<td>158</td>
<td>The The registering device’s ID is invalid</td>
</tr>
<tr>
<td>Cause Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>159</td>
<td>The caller’s device is not registered</td>
</tr>
<tr>
<td>160</td>
<td>The called party’s device is not registered</td>
</tr>
<tr>
<td>161</td>
<td>The registering device’s permissions have expired</td>
</tr>
<tr>
<td>162</td>
<td>The registering device has a duplicate alias</td>
</tr>
<tr>
<td>163</td>
<td>The call transport is not supported</td>
</tr>
<tr>
<td>164</td>
<td>The called device has a call in progress</td>
</tr>
<tr>
<td>165</td>
<td>The call has been routed to the gatekeeper</td>
</tr>
<tr>
<td>166</td>
<td>Cannot request a drop for others</td>
</tr>
<tr>
<td>167</td>
<td>The registering device is not registered with the gatekeeper</td>
</tr>
<tr>
<td>168</td>
<td>Unknown reason</td>
</tr>
<tr>
<td>169</td>
<td>Permission failure</td>
</tr>
<tr>
<td>170</td>
<td>Discovery permissions have expired</td>
</tr>
<tr>
<td>171</td>
<td>The device is not registered</td>
</tr>
<tr>
<td>172</td>
<td>No bandwidth available</td>
</tr>
<tr>
<td>173</td>
<td>Location not found</td>
</tr>
<tr>
<td>174</td>
<td>Security access denied</td>
</tr>
<tr>
<td>175</td>
<td>Quality of service not supported</td>
</tr>
<tr>
<td>176</td>
<td>Resources are exhausted</td>
</tr>
<tr>
<td>177</td>
<td>Invalid alias</td>
</tr>
<tr>
<td>178</td>
<td>Cannot unregister others</td>
</tr>
<tr>
<td>179</td>
<td>Quality of service control is not supported</td>
</tr>
<tr>
<td>180</td>
<td>Incomplete address</td>
</tr>
<tr>
<td>181</td>
<td>Registration permissions have expired</td>
</tr>
<tr>
<td>182</td>
<td>Call routed to SCN</td>
</tr>
<tr>
<td>183</td>
<td>Inconsistent alias</td>
</tr>
<tr>
<td>203</td>
<td>Call rejected at destination</td>
</tr>
<tr>
<td>208</td>
<td>Incorrect address</td>
</tr>
<tr>
<td>221</td>
<td>The far end is busy</td>
</tr>
<tr>
<td>222</td>
<td>The far end is not responding</td>
</tr>
</tbody>
</table>
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 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.

Table A-1  Inbound ports required on CMA system

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 80</td>
<td>HTTP web server, through which the web application displays and where Polycom endpoints post status messages</td>
</tr>
<tr>
<td>UPD 123</td>
<td>Network Time Protocol (NTP) listener</td>
</tr>
<tr>
<td>TCP135</td>
<td>Microsoft RPC listener</td>
</tr>
<tr>
<td>TCP/UPD 137</td>
<td>NetBIOS name service listener</td>
</tr>
<tr>
<td>TCP/UPD 139</td>
<td>NetBIOS SMB listener</td>
</tr>
<tr>
<td>TCP/UPD 161</td>
<td>SNMP listener</td>
</tr>
<tr>
<td>TCP 389</td>
<td>Directory services (LDAP)</td>
</tr>
<tr>
<td>TCP 443</td>
<td>HTTPS web server listener</td>
</tr>
<tr>
<td>TCP 700</td>
<td>Service monitor for redundant Polycom CMA servers</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 20</td>
<td>Used to FTP data to endpoints</td>
</tr>
<tr>
<td>TCP 21</td>
<td>Used to access the telnet interfaces on endpoints</td>
</tr>
<tr>
<td>TCP/UPD 23</td>
<td>Used to access a secondary telnet interface on endpoints</td>
</tr>
<tr>
<td>TCP/UPD 24</td>
<td>Used to send email messages to SMTP servers</td>
</tr>
<tr>
<td>TCP/UPD 25</td>
<td>Used to access domain name servers (DNS)</td>
</tr>
<tr>
<td>TCP 80</td>
<td>Used to access the web application on endpoints and MGCs, version 7.x and higher</td>
</tr>
<tr>
<td>TCP 135</td>
<td>Active Directory Single Signon (NetBios/NTLM)</td>
</tr>
<tr>
<td>TCP 137</td>
<td></td>
</tr>
<tr>
<td>TCP 139</td>
<td></td>
</tr>
</tbody>
</table>
Table A-2  Outbound ports required by Polycom CMA system

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/UPD 389</td>
<td>Used to access LDAP services</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Secure access to endpoint devices (SSL) including CMA Desktop</td>
</tr>
<tr>
<td>TCP 1205</td>
<td>Used to access MGCs for management and monitoring</td>
</tr>
<tr>
<td>TCP/UPD 1719</td>
<td>Used by the gatekeeper for H.323 datagrams</td>
</tr>
<tr>
<td>TCP/UPD 1720</td>
<td>Used by the gatekeeper for H.323 RAS messages</td>
</tr>
<tr>
<td>TCP/UPD 3268</td>
<td>Used to access the Active Directory Global Catalog</td>
</tr>
<tr>
<td>TCP 5001</td>
<td>Used to access MGCs for management and monitoring</td>
</tr>
<tr>
<td>TCP 5222</td>
<td>Presence server (XMPP)</td>
</tr>
</tbody>
</table>
The text input fields in each Polycom® Converged Management Application™ (CMA™) system screen accept basic ASCII, extended-ASCII (eASCII), or Unicode input as indicated in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data Format</th>
<th>Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Value: Owner</td>
<td>Unicode</td>
<td>Schedule</td>
</tr>
<tr>
<td>Filter Value: Conference Name</td>
<td>Unicode</td>
<td>Schedule</td>
</tr>
<tr>
<td>Conference Name</td>
<td>Unicode</td>
<td>Add/Edit Conference</td>
</tr>
<tr>
<td>Last Name</td>
<td>Unicode</td>
<td>Add/Edit Conference &gt; Add Participants</td>
</tr>
<tr>
<td>First Name</td>
<td>Unicode</td>
<td>Add/Edit Conference &gt; Add Participants</td>
</tr>
<tr>
<td>Name</td>
<td>Unicode</td>
<td>Add/Edit Conference &gt; Add Guest</td>
</tr>
<tr>
<td>Email</td>
<td>ASCII(1)</td>
<td>Add/Edit Conference &gt; Add Guest</td>
</tr>
<tr>
<td>Number</td>
<td>N/A</td>
<td>Add/Edit Conference &gt; Add Guest &gt; Dial-Out + IP</td>
</tr>
<tr>
<td>To</td>
<td>ASCII</td>
<td>Add/Edit Conference &gt; Email Notification</td>
</tr>
<tr>
<td>CC</td>
<td>ASCII</td>
<td>Add/Edit Conference &gt; Email Notification</td>
</tr>
<tr>
<td>BCC</td>
<td>ASCII</td>
<td>Add/Edit Conference &gt; Email Notification</td>
</tr>
<tr>
<td>Additional Notes</td>
<td>Unicode</td>
<td>Add/Edit Conference &gt; Email Notification</td>
</tr>
<tr>
<td>Filter Value: Name</td>
<td>ASCII</td>
<td>Device &gt; Admin/Monitor View</td>
</tr>
<tr>
<td>Filter Value: Alias</td>
<td>ASCII</td>
<td>Device &gt; Admin/Monitor View</td>
</tr>
<tr>
<td>Filter Value: Site</td>
<td>Unicode</td>
<td>Device &gt; Admin/Monitor View</td>
</tr>
<tr>
<td>Admin ID</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Find Device on Network</td>
</tr>
<tr>
<td>Password</td>
<td>ASCII(15)</td>
<td>Add/Edit Device &gt; Find Device on Network</td>
</tr>
<tr>
<td>System Name</td>
<td>ASCII(2)</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>eASCII</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>Serial Number</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>Software Version</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>HTTP URL</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>Numeric</td>
<td>Add/Edit Device &gt; Identification</td>
</tr>
<tr>
<td>DNS Name</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (E164)</td>
<td>0 through 9, *, and #</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (H323 ID)</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (URL)</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (Transport Address)</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (Party Number)</td>
<td>Numeric</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Alias Value (Unknown)</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; Addresses</td>
</tr>
<tr>
<td>Service Name</td>
<td>ASCII</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; Gateway</td>
</tr>
<tr>
<td>Dialing Prefix</td>
<td>Numeric</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; Gateway</td>
</tr>
<tr>
<td>Channels</td>
<td>Numeric</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; H320</td>
</tr>
<tr>
<td>Number Range</td>
<td>0 through 9 and '.' (dash)</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; H320</td>
</tr>
<tr>
<td>Service IP Address</td>
<td>0 through 9 and '.' (period)</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; H323</td>
</tr>
<tr>
<td>Alias</td>
<td>E164</td>
<td>Add/Edit Device &gt; MCU Services &gt; Add &gt; H323</td>
</tr>
<tr>
<td>Message Text</td>
<td>ASCII</td>
<td>Device &gt; Admin/Monitor View &gt; Send Message</td>
</tr>
<tr>
<td>Filter Value: Name</td>
<td>ASCII</td>
<td>Device &gt; Softupdate View &gt; Filter</td>
</tr>
<tr>
<td>Filter Value: Alias</td>
<td>ASCII</td>
<td>Device &gt; Softupdate View &gt; Filter</td>
</tr>
<tr>
<td>Filter Value: Site</td>
<td>Unicode(9)</td>
<td>Device &gt; Softupdate View &gt; Filter</td>
</tr>
<tr>
<td>Name</td>
<td>Unicode(5)</td>
<td>Add/Edit Conference Template</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Add/Edit Conference Template</td>
</tr>
<tr>
<td>RMX Profile Name</td>
<td></td>
<td>Add/Edit Conference Template</td>
</tr>
<tr>
<td>Talk Hold Time</td>
<td>Numeric x.x to y.y</td>
<td>Add/Edit Conference Template</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>From Address</td>
<td>ASCII</td>
<td>Conference Settings</td>
</tr>
<tr>
<td>SMTP Server</td>
<td></td>
<td>Conference Settings</td>
</tr>
<tr>
<td>Filter Value: First Name</td>
<td>Unicode</td>
<td>Users &gt; Attribute Filter</td>
</tr>
<tr>
<td>Filter Value: Last Name</td>
<td>Unicode</td>
<td>Users &gt; Attribute Filter</td>
</tr>
<tr>
<td>Filter Value: User ID</td>
<td>Unicode</td>
<td>Users &gt; Attribute Filter</td>
</tr>
<tr>
<td>First Name</td>
<td>Unicode(6)</td>
<td>Add/Edit User</td>
</tr>
<tr>
<td>Last Name</td>
<td>Unicode</td>
<td>Add/Edit User</td>
</tr>
<tr>
<td>User ID</td>
<td>Unicode</td>
<td>Add/Edit User; AND Login Screen</td>
</tr>
<tr>
<td>Password/Confirm Password</td>
<td>Unicode(7)</td>
<td>Add/Edit User; AND Login Screen</td>
</tr>
<tr>
<td>Email Address</td>
<td>Unicode(8)</td>
<td>Add/Edit User</td>
</tr>
<tr>
<td>Search Value</td>
<td>Unicode</td>
<td>Add Room &gt; search LDAP by First Name</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Add/Edit Room &gt; General Info</td>
</tr>
<tr>
<td>Email</td>
<td>Unicode(8)</td>
<td>Add/Edit Room &gt; General Info (display of LDAP email address or entry of a Local email address)</td>
</tr>
<tr>
<td>Filter Value: Device Name</td>
<td>ASCII</td>
<td>Global Address Book &gt; Attribute Filter</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII(10)</td>
<td>Add GAB User</td>
</tr>
<tr>
<td>E-164 Alias</td>
<td>0 through 9, *, and #</td>
<td>Add GAB User &gt; IP Video</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address format</td>
<td>Add GAB User &gt; IP Video</td>
</tr>
<tr>
<td>City Code</td>
<td>Numeric</td>
<td>Add GAB User &gt; ISDN Video</td>
</tr>
<tr>
<td>Number A</td>
<td>Numeric</td>
<td>Add GAB User &gt; ISDN Video</td>
</tr>
<tr>
<td>Number B</td>
<td>Numeric</td>
<td>Add GAB User &gt; ISDN Video</td>
</tr>
<tr>
<td>Extension</td>
<td>Numeric</td>
<td>Add GAB User &gt; ISDN Video</td>
</tr>
<tr>
<td>Old Password</td>
<td>ASCII(11)</td>
<td>Set GAB Password</td>
</tr>
<tr>
<td>New Password / Confirm</td>
<td>ASCII</td>
<td>Set GAB Password</td>
</tr>
<tr>
<td>Filter Value: Name</td>
<td>ASCII(2)</td>
<td>Provision Device Profiles</td>
</tr>
<tr>
<td>Filter Value: Created By</td>
<td>Unicode(12)</td>
<td>Provision Device Profiles</td>
</tr>
<tr>
<td>Admin Password</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; General Settings &gt; Security</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Meeting Password</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; General Settings &gt; Security</td>
</tr>
<tr>
<td>Country Code</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Video Network &gt; IP Network &gt; Gateway Number</td>
</tr>
<tr>
<td>Area Code</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Video Network &gt; IP Network &gt; Gateway Number</td>
</tr>
<tr>
<td>Gateway Number</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Video Network &gt; IP Network &gt; Gateway Number</td>
</tr>
<tr>
<td>Outside Line Dialing Prefix</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Video Network &gt; IP Network &gt; ISDN BRI Protocol</td>
</tr>
<tr>
<td>Camera 1 Name</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Cameras</td>
</tr>
<tr>
<td>Camera 2 Name</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Cameras</td>
</tr>
<tr>
<td>Camera 3 Name</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Cameras</td>
</tr>
<tr>
<td>Host Name</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; LAN Properties &gt; LAN Properties 1</td>
</tr>
<tr>
<td>Password</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Directory Servers</td>
</tr>
<tr>
<td>Number of digits in Extension</td>
<td>Numeric</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 1</td>
</tr>
<tr>
<td>International Dialing Prefix</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 1</td>
</tr>
<tr>
<td>Public Network Dialing Prefix</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 1</td>
</tr>
<tr>
<td>Public Network (same area code)</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 1</td>
</tr>
<tr>
<td>Private Network Dialing Prefix</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 1</td>
</tr>
<tr>
<td>If Area Code Equals</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 2</td>
</tr>
<tr>
<td>Dial Prefix</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; Dialing Rules 2</td>
</tr>
<tr>
<td>Contact Person</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Contact Number</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Contact Email</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Contact Fax</td>
<td>E164</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Tech Support</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>City</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>State/Province</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Country</td>
<td>ASCII</td>
<td>Add/Edit Provision Profile &gt; Global Services &gt; My Information</td>
</tr>
<tr>
<td>Software Update Key File</td>
<td>ASCII</td>
<td>Software Update Profile &gt; Upload Software Update</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Software Update Profile &gt; Upload Software Update</td>
</tr>
<tr>
<td>Filter Value: Name</td>
<td>ASCII(2)</td>
<td>Software Update Profiles &gt; Get Serial Numbers</td>
</tr>
<tr>
<td>Filter Value: Site</td>
<td>Unicode</td>
<td>Software Update Profiles &gt; Get Serial Numbers</td>
</tr>
<tr>
<td>Get Serial Numbers text box</td>
<td>ASCII</td>
<td>Software Update Profiles &gt; Get Serial Numbers</td>
</tr>
<tr>
<td>Filter Value: Name</td>
<td>ASCII</td>
<td>User Roles</td>
</tr>
<tr>
<td>Filter Value: Description</td>
<td>ASCII</td>
<td>User Roles</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII</td>
<td>User Roles &gt; Add/Edit Role</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>User Roles &gt; Add/Edit Role</td>
</tr>
<tr>
<td>Filter Value: Group Name</td>
<td>Unicode(13)</td>
<td>User Roles for LDAP Groups</td>
</tr>
<tr>
<td>Filter String</td>
<td>ASCII</td>
<td>Reports &gt; Gatekeeper Message Log</td>
</tr>
<tr>
<td>Filter Value: IP Address</td>
<td>IP Address</td>
<td>Reports &gt; IP Call Detail Records</td>
</tr>
<tr>
<td>Filter Value: System Name</td>
<td>ASCII(2)</td>
<td>Reports &gt; ISDN Call Detail Records</td>
</tr>
<tr>
<td>System Name</td>
<td>ASCII(14)</td>
<td>Server Settings &gt; Network</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address</td>
<td>Server Settings &gt; Network</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Subnet Mask</td>
<td>Server Settings &gt; Network</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>IP Address</td>
<td>Server Settings &gt; Network</td>
</tr>
<tr>
<td>DNS Server</td>
<td>IP Address</td>
<td>Server Settings &gt; Network</td>
</tr>
<tr>
<td>IP Address or DNS Name</td>
<td>ASCII</td>
<td>Server Settings &gt; System Time &gt; External NTP Server Time Synchronization</td>
</tr>
<tr>
<td>DB Server IP Address</td>
<td>IP Address</td>
<td>Server Settings &gt; Database</td>
</tr>
<tr>
<td>DB Server Port</td>
<td>Numeric</td>
<td>Server Settings &gt; Database</td>
</tr>
<tr>
<td>DB Instance Name</td>
<td>ASCII</td>
<td>Server Settings &gt; Database</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>LDAP Server IP Address or DNS Name</td>
<td>ASCII</td>
<td>Server Settings &gt; LDAP</td>
</tr>
<tr>
<td>LDAP User ID</td>
<td>Unicode(7)</td>
<td>Server Settings &gt; LDAP</td>
</tr>
<tr>
<td>LDAP User Password</td>
<td>Unicode(7)</td>
<td>Server Settings &gt; LDAP</td>
</tr>
<tr>
<td>Activation Key</td>
<td>ASCII</td>
<td>Server Settings &gt; Licenses</td>
</tr>
<tr>
<td>Virtual IP</td>
<td>IP Address</td>
<td>Server Settings &gt; Redundant Configuration</td>
</tr>
<tr>
<td>Server IP</td>
<td>IP Address</td>
<td>Server Settings &gt; Redundant Configuration</td>
</tr>
<tr>
<td>Gatekeeper Identifier</td>
<td>ASCII</td>
<td>Gatekeeper Settings &gt; Primary Gatekeeper</td>
</tr>
<tr>
<td>Gatekeeper Description</td>
<td>ASCII</td>
<td>Gatekeeper Settings &gt; Primary Gatekeeper</td>
</tr>
<tr>
<td>Alternate Gatekeeper ID</td>
<td>ASCII</td>
<td>Gatekeeper Settings &gt; Alternate Gatekeeper</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address</td>
<td>Gatekeeper Settings &gt; Alternate Gatekeeper</td>
</tr>
<tr>
<td>Port</td>
<td>Numeric</td>
<td>Gatekeeper Settings &gt; Alternate Gatekeeper</td>
</tr>
<tr>
<td>Priority</td>
<td>Numeric</td>
<td>Gatekeeper Settings &gt; Alternate Gatekeeper</td>
</tr>
<tr>
<td>Country Name (2 letter code)</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>State or Province Name</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Locality Name</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Organization Name</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Organizational Unit Name</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Common Name</td>
<td>ASCII(14)</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Email Address</td>
<td>ASCII</td>
<td>Security Settings &gt; Generate Certificate Request</td>
</tr>
<tr>
<td>Password / Verify Password</td>
<td>ASCII(15)</td>
<td>Security Settings &gt; Device Management Settings</td>
</tr>
<tr>
<td>Site Name</td>
<td>Unicode(9)</td>
<td>Dial Plan &gt; Sites &gt; Add/Edit Site</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; Sites &gt; Add/Edit Site</td>
</tr>
<tr>
<td>PBX Access Code</td>
<td>E164</td>
<td>Dial Plan &gt; Sites &gt; Add/Edit Site</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII</td>
<td>Dial Plan &gt; Site-Links &gt; Add/Edit Site-Link</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; Site-Links &gt; Add/Edit Site-Link</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII</td>
<td>Dial Plan &gt; Gatekeeper Regions &gt; Add/Edit Region</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; Gatekeeper Regions &gt; Add/Edit Region</td>
</tr>
<tr>
<td>Gatekeeper IP Address</td>
<td>IP Address</td>
<td>Dial Plan &gt; Gatekeeper Regions &gt; Add/Edit Region</td>
</tr>
<tr>
<td>Gatekeeper Identifier</td>
<td>ASCII</td>
<td>Dial Plan &gt; Gatekeeper Regions &gt; Add/Edit Region</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; General Info</td>
</tr>
<tr>
<td>Field</td>
<td>Data Format</td>
<td>Screen</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Prefix</td>
<td>ASCII</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; General Info</td>
</tr>
<tr>
<td>Insert between Prefix &amp; First number</td>
<td>E164</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Simplified Dialing</td>
</tr>
<tr>
<td>Insert between Phone number</td>
<td>E164</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Simplified Dialing</td>
</tr>
<tr>
<td>Append after full Dial string</td>
<td>E164</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Simplified Dialing</td>
</tr>
<tr>
<td>Login ID</td>
<td>ASCII</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Conference On Demand</td>
</tr>
<tr>
<td>Password</td>
<td>ASCII</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Conference On Demand</td>
</tr>
<tr>
<td>H.323 Network Service</td>
<td>ASCII</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Conference On Demand</td>
</tr>
<tr>
<td>RMX Profile Name</td>
<td>Unicode</td>
<td>Dial Plan &gt; Services &gt; Add/Edit Service &gt; Conference On Demand</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII</td>
<td>Dial Plan &gt; Dial Rules &gt; Add/Edit Rule &gt; General Information</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; Dial Rules &gt; Add/Edit Rule &gt; General Information</td>
</tr>
<tr>
<td>IP Address Pattern Data</td>
<td>ASCII</td>
<td>Dial Plan &gt; Dial Rules &gt; Add/Edit Rule &gt; Routing Action</td>
</tr>
<tr>
<td>Name</td>
<td>ASCII</td>
<td>Dial Plan &gt; LCR Tables &gt; Add/Edit LCR</td>
</tr>
<tr>
<td>Description</td>
<td>ASCII</td>
<td>Dial Plan &gt; LCR Tables &gt; Add/Edit LCR</td>
</tr>
<tr>
<td>Alert Note</td>
<td>ASCII</td>
<td>System Alerts &gt; Edit</td>
</tr>
</tbody>
</table>
### Index

**MCU and gateway dialing problems** 271

**A**
- Acknowledge Help command 35
- activation key, requesting 202
- activation keys, requesting 94, 98
- active conference. See conference
- Add Conference command 23
- Add Device command 53, 57, 60
  - adding
    - an alternate gatekeeper 208
    - conference templates 161
    - conferences 25
    - custom logos to the user interface 206
    - dial rules 246
    - gatekeeper regions 232
    - least-cost-routing tables 253
    - provisioning profiles 84, 86
    - rooms 150
    - services 239
    - site links 230
    - sites 220
    - system licenses 201
    - user roles 129
    - users to the global address book 147
    - users to the system 124
- adding manually
  - endpoints 72
  - MCUs 76
- address book. See global address book
- admin/monitor view commands
  - Clear Help 54
  - Delete Device 54
  - Edit Device 53
  - Manage Device 54
  - Manage User 54
  - Reboot Device 54
  - Send Message 54
  - View Device Details 53
- administering a redundant system 194

Adobe Flash Player 2
- advanced conference settings 37
  - editing 40
- alternate gatekeeper
  - adding 208
  - editing settings for 191, 208
- area codes, determining 251
- assigning
  - a lecturer 29
  - a video chairperson 29
  - user roles and devices 128
- audio-only conference 26
- automatic provisioning profiles
  - uploading for software updates 95, 99
- automatic refresh of system dashboard 132
- automatic software updates
  - uploading the image 95, 99
- auto-provisioning endpoints 216
- available commands, list of 21, 51

**B**
- backing up
  - system databases 137, 139
- backup files
  - copying 139
- bandwidth. See bit rate
- bit rate
  - setting for guest participants 28, 34
  - setting for internal participants 39
- bridge (MCU)
  - features field names 46
  - features, list of 22
  - forcing use of 38

**C**
- call detail records
  - IP call detail records, viewing and exporting 171
  - ISDN call detail records, viewing and exporting 171
  - overview of reports 169
call routing
setting up 13
Cancel Provision command 57
Cancel Update command 60
canceling
conferences 29
provisioning 89
software updates 101
capabilities, system, list of 1
CDR. See call detail records
chairperson
assigning 29
enabling 38
password for 38
changing
advanced conference settings 40
alternate gatekeeper settings 208
conference information 30
conference templates 162
devices 79
dial rules 247
gatekeeper regions 233
least-cost-routing tables 253
participant dial options 31
participant endpoint settings 31
password for the global address book 149
permissions for a user role 130
primary gatekeeper settings 207
provisioning profiles 85, 87
room dial options 32
room endpoint settings 32
rooms 151
security settings for https 211
services 240
site links 230
site settings 227
system network settings 195
system time settings 196
user information 125
user information in the global address book 148
checking the status of device provisioning 88
Clear Help command 54
Clear Status command 57, 60
clearing
device help requests 81
gatekeeper message log events 167
status of device provisioning 89
cloning provisioning profiles 85, 87
closing the CMA system 3
command categories
admin/monitor view commands 53
softupdate view commands 60
commands
Acknowledge Help 35
Add Conference 23
Add Device 53, 57, 60
Cancel Provision 57
Cancel Update 60
Clear Help 54
Clear Status 57, 60
conference 23
Connect/Disconnect participant 35
Delete Conference 23
Delete Device 54
Edit Conference 23
Edit Device 53
list of 21, 51
Manage Conference 24
Manage Device 54
Manage User 54
Monitor Conf View 23
Mute/Unmute Participant 35
Provision 57
Reboot Device 54
Refresh View 23
Remove Participant 35
Schedule Conf View 23
Send Message 35, 54
Software Update 60
System Management 135
Terminate Conference 24
View Device Details 53
commands, dashboard
Refresh 134
Restart 134
Shutdown 134
System Log Files 134
conference commands 23
conference details
conference details field names 42
displaying 22
conference features field names 44
conference list field names 41
conference on demand
troubleshooting 272
conference on demand service 234
conference rooms
adding 28
setting dial options for 32
setting endpoints for 32
conference settings
ingitting 40
conference settings. See settings
conference templates
adding 161
deleting 162
editing 162
overview of 153
setting up 15
viewing list of 161
conferences
assigning password for 37
deleting 29
displaying information about 132
features, list of 22
list of conferences 21, 22
list of notes for 22
managing 33
overview of conference settings 159
scheduling 25
sending email notification for 29
setting to audio only 26
setting to recurring 25
configuration, system
displaying information about 133
configuring
a redundant system 192
an external database 13
an LDAP connection 13
endpoints 216
redundancy 10
configuring devices 62
Connect/Disconnect Participant command 35
connected users
displaying information about 133
connecting to the serial console 138
connection speed
setting for guest participants 28, 34
setting for internal participants 39
console, connecting to 138
continuous presence mode 38
copying
database backup files 139
provisioning profiles 85, 87
country codes, determining 251
creating
conferences 25
dial rules 246
least-cost-routing tables 253
custom
custom dialing rules, examples of 245
custom logo, adding to the user interface 206
Custom Date filter 21
customizing the user interface 206

D
dashboard 131
dashboard commands
Refresh 134
Restart 134
Shutdown 134
System Log Files 134
data plus video stream 39
database, external
backing up 137
integrating with the system 198
restoring 142
database, external, configuring 13
database, internal
reverting to 199
databases
backing up 139
copying backup files 139
restoring, overview of 141
databases, internal
backing up 137
restoring 141
defaults
for dial rules 243
for dial-plan settings 184
defining
gatekeeper message log settings 167
Delete Conference command 23
Delete Device command 54
deleting
conference templates 162
conferences 29
devices 80
gatekeeper message log events 167
gatekeeper regions 233
least-cost-routing tables 253
provisioning profiles 86, 87
rooms 151
services 240
site links 231
sites 227
user roles 130
users 126
users from the global address book 148
deleting a conference 23
details of conference, displaying 22
determining
area codes 251
country codes 251
weighted cost 252
device commands
Add Device 53, 57, 60
device details
  alias 74, 105
  audio protocol 107
  available to schedule 75, 104
  call type 107
  capabilities enabled 74, 105
  cause code 107
  description 73
  device local time 106
  encryption 107
  endpoint ISDN type 106
  errors 108
  far site name 107
  far site number 107
  gatekeeper registration 105
  GDS registration 105
  GK registration timeout 106
  HTTP port 73
  HTTP URL 73
  IP address 53, 72, 103
  ISDN assignment type 106
  ISDN line status type 106
  ISDN video number 74, 103
  last GK registration 106
  monitoring level 75, 104
  name 72, 73
  owner 103
  serial number 73, 104
  site 73, 104
  software version 73, 104
  supported protocols 74, 104
  type 72
  video format 107
  video protocol 107
  warnings 108
device details, viewing 71
device list field names 52
device lists
  list of provisioning details 86
  list of serial numbers for 93, 97
device summary
  name 53, 103
  type 53, 103
devices
  assigning to users 128
  canceling provisioning for 89
  checking provisioning status for 88
  clearing a help request for 81
  clearing provisioning status for 89
  configuring 62
  deleting 80
  device details field names 103
displaying information about 132
  displaying information about management of 132
  editing information about 79
  MCU device details field names 110
  provisioning 88
  provisioning details field names 108
  scheduling software updates for 100
  sending messages to 81
  setting passwords for 70
  softupdate details field names 109
  video feed for 80
See also endpoints
devices, managing for participants 35
dial options
  editing 31
  setting 38
  setting for guest participants 28, 34
dial plan services
  conference on demand service 234
  gateway service 236
  MCU service 238
  overview of 234
  simplified dialing service 235
dial plan settings
  default values for 184
  overview of 180
dial rules
  adding 246
  default 243
  editing 247
  enabling/disabling 247
  examples of custom rules 245
  overview of 240
  pattern types 243
  routing actions 244
  rule components 243
  viewing list of 245
dial type
  setting for guest participants 28, 34
dial-in option 38
dial-out option 38
Directory Overview screen 4
directory services
  setting up 15
disabling/enabling dial rules 247
disconnecting/connecting a participant 35
displaying
  conference templates list 161
  configuration information 133
  connected-users information 133
  device details 71
device information 132
 device-management information 132
gatekeeper message log 167
 global address book 147
 IP call detail records 171
 ISDN call detail records 171
 license information 132
 MCU information 132
 network-usage information 133
 rooms list 150
 services information 133
 site link statistics 169
 site statistics 168
 system log files 176
 system-usage information 133
 today’s conferences 132
 user roles list 129
 downloading software updates 94, 98

today’s conferences 132

E
Edit Conference command 23
Edit Device command 53
ingestion
 advanced conference settings 40
 alternate gatekeeper settings 208
 conference information 30
 conference templates 162
 devices 79
 dial rules 247
 gatekeeper regions 233
 least-cost-routing tables 253
 participant dial options 31
 participant endpoint settings 31
 password for the global address book 149
 permissions for a user role 130
 primary gatekeeper settings 207
 provisioning profiles 85, 87
 room dial options 32
 room endpoint settings 32
 rooms 151
 security settings for https 211
 services 240
 site links 230
 site settings 227
 system network settings 195
 system time settings 196
 user information 125
 user information in the global address book 148
 email notifications 29
 enabling a chairperson 38
 enabling/disabling dial rules 247
 endpoints
adding manually 72
 auto-provisioning 216
 editing settings for 31
 sending messages to 35
 setting common passwords for 216
 setting passwords for 70
 third-party 61
 See also devices
entering the system license number 202
exporting
 gatekeeper message log 167
 IP call detail records 171
 ISDN call detail records 171
 system log files 176
 external database
 integrating with the system 198
 external database, configuring 13
 external databases. See databases and database, external

F
failover, initiating in a redundant system 205
features
 bridge (MCU) 22
 list of conference 22
 features, system, list of 1
 feed, viewing for a video device 80
 field names
 bridge (MCU) features 46
 conference details 42
 conference features 44
 conference list 41
 device details 103
 device list 52
 MCU device details 110
 participant details 47
 participant settings 48
 participants 47
 participants list 50
 provisioning details 108
 softupdate details 109
 fields
 input requirements for 6
 filtering
 overview of 6
 filters
 Custom Date 21
 Future Only 21
 Ongoing Plus 21
 Today Only 21
 Today Plus 22
 Yesterday Plus 22
first-time setup, resetting during a recovery setup 142
forcing MCU usage 38
Future Only filter 21

G
gatekeeper message log
  clearing events from 167
  defining messages to be logged 167
  overview of 165
  pausing and restarting 168
  viewing and exporting 167
gatekeeper regions
  adding 232
  deleting 233
  editing 233
gatekeeper settings
  editing for alternate gatekeeper 208
  editing for primary gatekeeper 207
  for alternate gatekeeper, overview of 191
  for primary gatekeeper, overview of 189
  overview of 180
gatekeepers
  adding alternate 208
  gatekeeper regions, overview of 231
  overview of 188
  viewing gatekeeper regions list 232
gateway dialing, troubleshooting 271
gateway service 236
global address book
  adding users to 147
  deleting users from 148
  editing the password for 149
  editing user information in 148
  overview of 145
  viewing 147
guest participants
  adding 27, 34
  setting bit rate for 28, 34
  setting dial options for 28, 34
  setting dial type for 28, 34

H
help request, clearing for a device 81
help, acknowledging 35
https, implementing 211

I
implementing
  a redundant system 203
  https 211
  initiating failover in a redundant system 205
input requirements for fields
  requirements for field inputs
    ASCII-only fields 6
integrating
  an external database 198
  an LDAP server 199
  LDAP 187
internal database, reverting to 199
internal databases. See databases and databases, internal
IP call detail records
  viewing and exporting 171
ISDN call detail records
  viewing and exporting 171

K
key for software activation, requesting 202
keys for software activation, requesting 94, 98

L
LCR. See least-cost routing (LCR)
LDAP 128
  integrating an LDAP server 199
  integrating LDAP 187
LDAP connection, configuring 13
least-cost routing (LCR)
  determining area codes for 251
  determining country codes for 251
  determining weighted cost for 252
least-cost-routing (LCR) tables
  adding 253
  deleting 253
  editing 253
  examples of 249
  overview of 248
  viewing list of 252
lecturer, assigning 29
licenses
  displaying information about 132
licenses, system
  adding 201
  entering number for 202
licensing the system 12
link statistics for a site
  overview of 169
  viewing 169
links for a site
  adding 230
as part of the site topology 181
deleting 231
editing 230
viewing list of 229
lists
filtering, overview of 6
of bridge (MCU) features 22
of commands 21, 51
of conference features 22
of conference notes 22
of conference templates 161
of conferences 21, 22, 41
of device serial numbers 93, 97
of devices 52
of dial rules 245
of gatekeeper regions 232
of least-cost-routing tables 252
of participant details 22
of participants 22, 50
of provisioning details 86
of rooms 150
of services 238
of site links 229
of sites 220
of system features and capabilities 1
of user roles 129
of users 123
logging into the CMA system 2
logging out of the CMA system 3
logo, adding to the user interface 206
logs
gatekeeper message log 165
system log files 174, 176
M
Manage Conference command 24
Manage Device command 54
Manage User command 54
management settings, overview of 180
managing
active conferences 33
participant devices 35
manual additions
endpoints 72
MCUs 76
MCU
features field names 46
forcing use of 38
list of features 22
MCU (Multipoint Control Unit)
definition 261
MCU device details
channels 77, 110
international prefix 78, 111
LCR table 77, 110
local area codes 78, 111
local prefix 77, 111
non-local prefix 78, 111
number range 77, 110
priority 78, 111
service name 77, 110
MCU dialing, troubleshooting 271
MCU service 238
MCUs
adding manually 76
displaying information about 132
MCU device details field names 110
menus
System Management 134
message, sending to a device 81
messages, sending 35
mode, T.120 40
modes, video
continuous presence mode 38
setting 38
switching mode 38
modifying
advanced conference settings 40
alternate gatekeeper settings 208
calendar information 30
calendar templates 162
devices 79
dial rules 247
gatekeeper regions 233
least-cost-routing tables 253
participant dial options 31
participant endpoint settings 31
password for the global address book 149
permissions for a user role 130
primary gatekeeper settings 207
provisioning profiles 85, 87
room dial options 32
room endpoint settings 32
rooms 151
security settings for https 211
services 240
site links 230
site settings 227
system network settings 195
system time settings 196
user information 125
user information in the global address book 148
Monitor Conf View command 23
Monitor Conferences screen 4
monitoring conf view 22
multipoint conference
definition 262
multisite links
definition 262
Muting/Unmuting Participant command 35

N
network settings, editing 195
network usage
displaying information about 133
notes, list of conference 22
number for system license, entering 202

O
Ongoing Plus filter 21
open ports
list of 275

P
participant field names
participant details field names 47
participant settings field names 48
participants list field names 50
participants
adding guest 27, 34
connecting/disconnecting 35
list of 22
list of, details 22
managing devices for 35
muting/unmuting 35
removing 35
setting endpoints for 31
participants field names
passwords
editing the global address book password 149
for chairperson 38
for conference 37
setting for endpoints 216
pattern types for a dial plan 243
pausing and restarting
gatekeeper message log 168
People + Content 39
point-to-point calls
troubleshooting 270
ports used by the SE200
list of 276
primary gatekeepers
ingesting settings for 207
overview of 189
Provision command 57
provision view commands
Cancel Provision 57
Clear Status 57
Provision 57
provisioning
canceling 89
provisioning details field names 108
starting 88
provisioning details
failure reason 109
last attempt date/time 109
last profile applied 108
log message 109
pending profile 108
provisioning status 108
scheduled 108
provisioning profiles
adding 84, 86
cloning 85, 87
deleting 86, 87
inging 85, 87
viewing list of 86
proxy, definition 262

R
Reboot Device command 54
records
IP call detail records 171
ISDN call detail records 171
recovery operations
overview of 142
recurring conferences 25
redundancy, configuring 10
redundant system
administering 194
configuring 192
implementing 203
initiating failover in 205
Refresh command 134
Refresh View command 23
refresh, automatic, of system dashboard 132
regions in the site topology 180
regions, gatekeeper
adding 232
deleting 233
ing 233
viewing 232
registration
troubleshooting problems with 267
Index

Remove Participant command 35
removing
  conference templates 162
  conferences 29
  devices 80
gatekeeper message log events 167
gatekeeper regions 233
least-cost-routing tables 253
provisioning profiles 86, 87
rooms 151
services 240
site links 231
sites 227
user from the global address book 148
user roles 130
users 126
removing a conference 23
reports
  call detail record reports 169
request for help, clearing for a device 81
requesting
  software activation key 202
requesting update activation keys 94, 98
requirements, system 2
requirements, system, list of 2
resetting first-time setup during a recovery operation 142
resources
  See also rooms
Restart command 134
restarting
  the gatekeeper message log 168
  the system 143
restoring
  databases, overview of 141
  external database 142
  internal databases 141
reverting to an internal database 199
roles, user
  adding 129
  deleting 130
  editing permissions for 130
  overview of 115, 128
  viewing list of 129
rooms
  adding 28, 150
  deleting 151
  editing 151
  overview of 149
  setting dial options for 32
  setting endpoints for 32
  viewing list of 150
routing
  routing actions for a dial plan 244
S
  Schedule Conf View command 23
  schedule conference view 21
  scheduling a conference 25
  scheduling software updates 100
searching
  users 123
security settings
  editing for https 211
  overview of 180
Send Message command 35, 54
sending a message to a device 81
serial console, connecting to 138
serial numbers for devices to be updated 93, 97
servers
  initiating failover in a redundant system 205
  LDAP 199
  settings, overview of 179
  updating software for 217
services
  adding 239
  deleting 240
  displaying information about 133
  editing 240
  viewing list of 238
services, dial plan
  conference on demand service 234
  gateway service 236
  MCU service 238
  overview of 234
  simplified dialing service 235
setting
  common passwords for endpoints 216
setting up
  conference templates 15
  directory services 15
  video call routing 13
settings
  advanced 37
  advanced conference settings 40
  alternate gatekeeper settings 191
  chairperson password 38
  conference password 37
  conference settings 139
  connection speed 39
  dial options 38
  dial plan settings 180, 184
  enable chairperson 38
forced MCU usage
gatekeeper settings
management settings
network settings
People + Content
primary gatekeeper settings
security settings
security settings for https
server settings
system time settings
T.120 mode
video mode
Shutdown command
shutting down the system
simplified dialing service
site link statistics
overview of
viewing
site links
adding
deleting
editing
overview of
place of in the site topology
viewing list of
site settings, editing
site statistics
overview of
viewing
site topology
overview of
regions in
site links in
sites in
subnets in
sites
adding
deleting
overview of
view graphical topology
viewing list of
softupdate
overview of
softupdate details field names
softupdate details
failure reason
last attempt date/time
log message
scheduled
softupdate status
softupdate view commands
  Cancel Update
software
  requesting activation key for
  updating for the server
Software Update command
software updates
  canceling
  downloading
  overview of
  scheduling
See also softupdate
SQL server database. See database, external
starting
  the gatekeeper message log
  the system
starting the CMA system
statistics
  site link statistics, overview of
  site statistics, overview of
  viewing site link statistics
  viewing site statistics
status of device provisioning
  checking
  clearing
stopping
  provisioning
  software updates
subnets, place of in the site topology
supported third-party endpoints
switching mode
system configuration
  displaying information about
system dashboard
system features and capabilities, list of
system integration with external database
system licenses
  adding
  entering number for
system log files
  overview of
  viewing and exporting
System Log Files command
system login
system management commands
system management menu
system network settings, editing
system requirements
system requirements, list of
system setup menu
Index

overview of 179
system time settings, editing 196
system usage
  displaying information about 133
system views 5
system, licensing 12

T
T.120 mode 40
templates, conference
  adding 161
  deleting 162
  editing 162
  overview of 153
  setting up 15
  viewing list of 161
Terminate Conference command 24
third-party endpoints 61
time settings, editing 196
Today Only filter 21
Today Plus filter 22
topology
  of sites 219
  overview of 180
  regions in 180
  site links in 181
  sites in 181
  subnets in 181
troubleshooting 271
  conference on demand problems 272
  point-to-point call problems 270
  registration problems 267

U
unmuting/muting a participant 35
updates, software
  canceling 101
  downloading 94, 98
  overview of 67
  requesting activation keys for 94, 98
  scheduling 100
See also softupdate
updating server software 217
uploading the software image 95, 99
usage
  displaying information about system usage 133
  displaying network-usage information 133
user
  search for a 123
user interface, adding a custom logo to 206
user roles
  adding 129
  deleting 130
  editing permissions for 130
  overview of 115
users
  adding to the global address book 147
  adding to the system 124
  assigning roles and devices to 128
  deleting 126
  displaying information about connected users 133
  editing information about 125
  editing information about in the global address book 148
  overview of 115
  roles for 128
  searching list of 123

V
video call routing
  setting up 13
video chairperson, assigning 29
video endpoints. See devices and endpoints
video feed, viewing for a device 80
video modes
  continuous presence mode 38
  setting 38
  switching mode 38
video plus data stream 39
view
  graphical site topology 219
View Device Details command 53
view_graphical_site_topology 219
viewing
  conference templates list 161
  configuration information 133
  connected-user information 133
  device details 71
  device information 132
  device serial numbers list 93, 97
  device-management information 132
  dial rules list 245
  gatekeeper message log 167
  gatekeeper regions list 232
  global address book 147
  IP call detail records 171
  ISDN call detail records 171
  least-cost-routing tables list 252
  license information 132
  MCU information 132
network-usage information 133
provisioning list and details 86
rooms list 150
services information 133
services list 238
site link statistics 169
site links list 229
site statistics 168
sites list 220
status of device provisioning 88
system log files 176
system-usage information 133
today’s conferences 132
user roles list 129

video feed for a device 80
views
monitor conf 22
schedule conference view 21

W
warnings 108
weighted cost, determining 252
workspaces in the CMA system 4

Y
Yesterday Plus filter 22