Operations Guide

8.1.0 | December 2013 | 3725-72104-001E

Polycom® RealPresence® Resource Manager System

Contents

Getting Started 22

Conference Scheduling 38

Network Device Management 246

User Management 277

System Configuration 323

Getting Started

This section provides on overview of system features and configuration:

Polycom RealPresence Resource Manager Overview

System Configuration

Polycom RealPresence Resource Manager Overview

This chapter provides an overview of the Polycom® RealPresence ® Resource Manager system and includes these topics:

RealPresence Resource Manager System Features and Capabilities

The RealPresence Resource Manager system is an integrated scheduling and device management platform for video conferencing that can include these features:

- Endpoint management, including provisioning, updating, monitoring, and troubleshooting
- Conference scheduling and monitoring on both RealPresence Resource Manager system resources and the Polycom DMA system (when integrated with the RealPresence Resource Manager system)
- Conference, network device, and system monitoring and management including network typology by geography and visual alarm reporting
- Directory and user management including address books and presence
- The Polycom CMA Desktop client for Windows and MAC operating systems—an easy-to-use video and audio conferencing application that lets your users see and hear the people they call on their desktop system.
- Endpoint provisioning allows you to edit endpoint settings for the endpoints registered to the RealPresence Resource Manager. Polycom endpoints can take advantage of the dynamic (automatic) provisioning based on provisioning rules. For legacy and third-party endpoints, you can manually schedule provisioning profiles to be sent at intervals you define.
- Dynamic software updates for dynamically-managed Polycom endpoint systems and scheduled software updates for third-party and legacy endpoints.
- Firewall management capabilities which enable video conferencing across firewalls.
- Access to user and room directories for on-demand and scheduled calls. Directory services include:

    - ➢ Presence and contact list functionality for dynamically-managed endpoints (except for RealPresence Mobile clients).
    - ➢ Global Address Book for a single directory structure or Multiple Address Books for multiple managed directories.
    - ➢ H.350 and LDAP directory functionality. H.350 defines a directory services architecture for multimedia conferencing for H.323, H.320, SIP and generic protocols.
- Device monitoring and management, including bridges and access controllers.
- An optional high-availability, redundant management server configuration.

Polycom RealPresence Resource Manager System

The RealPresence Resource Manager system supports up to 10,000 managed devices. It integrates with the DMA 7000 system for call control via H.323 gatekeeper and SIP proxy functions.

The RealPresence Resource Manager system is available in optional High Availability configurations without external database requirements.

The RealPresence Resource Manager system has the following options available (additional charges may apply):

- Integration with a corporate directory
- Integration with Polycom DMA 7000 systems for Virtual Meeting Room (VMR) management and scheduling of virtualized MCU resources
- Multi-tenant management
- Programmatic access through Application Programmers Interfaces (APIs)

Minimum System Requirements

The *Polycom RealPresence Resource Manager System Release Notes* describe the minimum system requirements for your RealPresence Resource Manager system. To find the most current *Release Notes, go* to www.support.polycom.com and navigate to the RealPresence Resource Manager system product page.

Working in the RealPresence Resource Manager System

These topics includes some general information you should know when working in the RealPresence Resource Manager system. It includes these topics:

- Log Into the RealPresence Resource Manager System on page 25
- Field Input Requirements on page 26
- Filter and Search a List on page 26

- Change a Password on page 28
- Log Out of the Polycom RealPresence Resource Manager System on page 29
- Restart or Shut Down a Polycom RealPresence Resource Manager System on page 29
- Emergency Shutdown of a Polycom RealPresence Resource Manager System on page 30

Log Into the RealPresence Resource Manager System

To log into the RealPresence Resource Manager system web interface, you need:

- Microsoft Internet Explorer® 8.0 or 9.0, Mozilla FireFox® 11 or higher, Apple Safari 10.6 or 10.7, or Google Chrome 17 or higher.
- Adobe® Flash® Player 9.x or 10.x
- The IP address or host name of the RealPresence Resource Manager system server and your username, password, and domain.

Note

The RealPresence Resource Manager system user interface is best viewed with an SXGA display resolution of at least 1280x1024 pixels. The minimum support display resolution is XGA 1024x768 pixels.

Generally, you get three opportunities to enter the correct password. After three failed attempts, the system returns an error message.

To log into a RealPresence Resource Manager system

1 Open a browser window and in the **Address** field enter the RealPresence Resource Manager system IP address or host name.

  - ➢ If prompted to install the Adobe Flash Player, click **OK.**
  - ➢ If you receive an HTTPS **Security Alert**, click **Yes**.
  - ➢ If you see a login banner, click **Accept** to accept the terms and continue.

  If you cannot connect to the system, there may be certificate issues.

2 When the RealPresence Resource Manager system **Log In** screen appears, enter your **Username** and **Password**.

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

4 Click **Login**.

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

If you log in as an administrator, you see the RealPresence Resource Manager system **Dashboard**.

For more information about roles and the functionality associated with roles, see Default System Roles and Permissions on page 282.

Field Input Requirements

While every effort was made to internationalize the RealPresence Resource Manager system, not all system fields accept Unicode entries. If you work in a language other than English, be aware that some RealPresence Resource Manager system fields may accept only ASCII or extended ASCII characters.

Filter and Search a List

In the RealPresence Resource Manager system interface, information is often summarized in lists or grids.

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

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

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

However, if the RealPresence Resource Manager system is integrated with an Active Directory, the RealPresence Resource Manager system uses the LDAP search function for searches of the directory. LDAP searches are prefix-searches that include an appended wildcard. In this case, when you enter a search string, the system looks for that search string only at the beginning of the indexed fields.

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

```
Barbara
Smithe
Bar
Smi
```

To optimize LDAP searches, the RealPresence Resource Manager system (and its dynamically-managed endpoints) searches only indexed LDAP fields and a limited set of attributes. The attributes include:

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

These are the requested attributes to be returned by the search:

```
Sn
Givenname
```

```
Mail
Ou
Objectguid
Telephonenumber
Cn
Samaccountname
Memberof
Displayname
Objectclass
Title
localityName
department
```

Managing Bandwidth

The RealPresence Resource Manager system manages the bandwidth between sites and the bandwidth for calls that it schedules within the gatekeeper region it services. The RealPresence Resource Manager supports using an external gatekeeper only, typically a Polycom DMA system.

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

- **The maximum bit rate for a call at a site.** Set it by editing the site, selecting **Routing/Bandwidth**, and setting the **Call Max Bit Rate**.
- **The total bandwidth between sites.** The link type and bandwidth are parameters of the site links between two sites. Set it by editing the site link.
- **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 RealPresence Resource Manager 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 RealPresence Resource Manager system only allows a connection speed when it is within the parameters set for the site link.

  - ➢ Endpoints 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 endpoint**. These values are parameters of the endpoint. For endpoints in dynamic management mode, these values are provisioned as part of an Admin Config provisioning profile. For endpoints operating in scheduled management mode, these values can be provisioned with a scheduled provisioning profile or modified at the endpoint itself.

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

Change a Password

For local users, RealPresence Resource Manager system password requirements (for example, password length and password age) are managed by the RealPresence Resource Manager system administrator. For enterprise users, RealPresence Resource Manager system password requirements are managed by Microsoft Active Directory.

To change your system password

1. Click Settings in the top-right corner of the page.
2. In the Settings dialog box, click **Change Password**.
3. Enter your **Old Password**.
4. Enter a **New Password**.
5. Confirm the new password and click **OK**.

Log Out of the Polycom RealPresence Resource Manager System

To log out of the RealPresence Resource Manager system

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

Restart or Shut Down a Polycom RealPresence Resource Manager System

You have several options for an orderly shutdown or restart of a RealPresence Resource Manager system in non-emergency situations.

The options for an orderly shutdown or restart of the system include:

- Use the **Shutdown** option on the user interface when you must disconnect the RealPresence Resource Manager system server for some reason; for example, to move it. All RealPresence Resource Manager system functionality is stopped during a **Shutdown**.

- If the system interface is not available and you must shut down the system, press once (but do not hold) the power switch on the RealPresence Resource Manager system server. This is equivalent to selecting the **Shutdown** option described previously.
- Use the **Restart** option on the user interface when you must cycle the RealPresence Resource Manager system for some reason; for example, if the system locks up or loses connection with Active Directory.

If you have access to the RealPresence Resource Manager system user interface, you can also stop future scheduled conferences from starting automatically and wait for active conferences to end before performing an orderly shut down or restart of the system.

During a restart, the system will drop all IP conferences. In general, ISDN conferences will not drop.

To restart or shut down a RealPresence Resource Manager system

1. (Optional) To stop future scheduled conferences from starting before you perform the restart or shutdown:

   a. Go to **Admin > Dashboard**.

   b. Monitor the **Today's Conferences** section to determine when all active conferences are completed.

2. Go to **Admin > Dashboard** and click **Restart** or **Shutdown** , as required.

   In a redundant RealPresence Resource Manager system configuration, if you requested a shutdown of the primary server, the system displays a warning indicating that it is initiating a failover.

   If you select **Restart**, it may take the RealPresence Resource Manager system up to 10 minutes to shutdown and then restart all server processes.

Emergency Shutdown of a Polycom RealPresence Resource Manager System

You have two options to perform an emergency shutdown of a RealPresence Resource Manager system. Use these options only when you must immediately cut power to the server.

- Press and hold the power switch on the RealPresence Resource Manager system server.
- Pull the system power cord.

After an emergency shutdown (that is when you press and hold the power switch, or you pull the system cord, or you lose power to the system), a system battery may continue to cache information until the battery runs out. In this case, the system enters an error state. To recover, you must connect a keyboard and monitor to the RealPresence Resource Manager system and boot the system to clear the error message. Then the system can begin recovery.

System Configuration

This chapter describes the configuration tasks that may be required, based on your system design and installation, to complete your implementation of a Polycom® RealPresence® Resource Manager system after **First Time Setup**. It includes these topics:

- Add DNS SRV Record for RealPresence Resource Manager System Services on page 31
- Configure the Connection to an External Enterprise Directory on page 32
- Configure Redundancy on page 32
- Set Up Site Topology on page 32
- Integrate with a Polycom DMA System on page 33
- Set Up Endpoint Management on page 33
- Set Up Conference Templates on page 34
- Set Up Directory Services on page 34
- Set Up a Certificate for the RealPresence Resource Manager System on page 35
- Distribute Polycom Applications on page 35

Add DNS SRV Record for RealPresence Resource Manager System Services

You must configure the DNS server, if you wish it to resolve queries for the RealPresence Resource Manager system by the RealPresence Resource Manager system's host name or IP address.

We recommend that the DNS server be configured to find the RealPresence Resource Manager system by its fully qualified domain name (FQDN). This ensures that client systems running Polycom CMA Desktop, RealPresence Mobile, and RealPresence m100 can access the RealPresence Resource Manager system.

The DNS should also have entries for your Active Directory server (if different from the DNS).

To dynamically manage endpoints (which includes dynamic provisioning, dynamic software update, and presence) right out-of-the-box, they must be able to automatically discover the RealPresence Resource Manager system.

This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager 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 0 443 Access5.customerdomain.com
```

For more information about DNS, DNS records, and how DNS works, see Microsoft Technet (http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx).

Support of Multiple Provisioning Servers

The SRV record must point to the Provisioning Server (RealPresence Resource Manager system) that endpoints will use for auto discovery for Dynamic Provisioning. Two or more provisioning servers may co-reside on a network; however only one may be used for DNS-based discovery of provisioning services.

If more than one provisioning server is used within a environment there is no knowledge or coordination between these environments including, but not limited to:

- No shared directory services
- No shared management or provisioning services
- No shared scheduling
- No shared licenses

Configure the Connection to an External Enterprise Directory

If during **First Time Setup** you did not configure your RealPresence Resource Manager system to use an enterprise directory, but need to do so now, see Understanding Directories on page 400.

Connecting to an enterprise directory allows users to enter their network usernames and password to log into RealPresence Resource Manager system. It also allows users to access the enterprise directory when selecting conference participants.

Configure Redundancy

You can install the RealPresence Resource Manager system in a fault-tolerant, high-availability, redundant configuration.

A redundant RealPresence Resource Manager system configuration requires the installation of two RealPresence Resource Manager system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses. Once the two system servers are installed, see System Redundancy on page 447 to finish implementing redundancy.

Set Up Site Topology

The video call routing setup includes site topology and bandwidth management.

You can perform the following tasks:

- 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. You can also define links between sites (site links).

- For each site, define the subnets in which the video endpoint systems are deployed. It is important that the IP addresses used by the endpoints belong to only one subnet at a site.

For more information, see Setting Up Site Topology on page 369.

Integrate with a Polycom DMA System

Polycom recommends integrating your RealPresence Resource Manager system with a Polycom DMA system for both call manager (gatekeeper) and conference manager services.

For more information, see Managing a DMA System on page 263.

Set Up Endpoint Management

The RealPresence Resource Manager system allows you to manage endpoints in two ways:

- Scheduled Management of Endpoints (Polycom and Third-Party) on page 33
- Dynamic Management of Endpoints (Polycom Only) on page 33

Scheduled Management of Endpoints (Polycom and Third-Party)

Scheduled management allows you to push software updates and provisioning profiles to endpoints at intervals that you define.

Scheduled management uses server-to-client communication over HTTP. This management technique is more appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.

For more information about scheduled management methods, see Scheduled Endpoint Management on page 122.

Dynamic Management of Endpoints (Polycom Only)

Dynamic management allows the endpoint to poll the RealPresence Resource Manager automatically to get dynamic provisioning profiles (configuration settings) and software updates on a regular basis.

Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is available:

- Only for Polycom endpoints.
- When your system is integrated with an enterprise directory.
- When Polycom endpoints are able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager.

In dynamic management mode, when a endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package or provisioning profile. If a either is found, the package is sent in XML format over a secure HTTPS connection.

Endpoints do not poll the system if they are in a call. They restart polling after the call ends.

For more information about dynamic management methods, see Understanding Dynamic Endpoint Management on page 156.

Set Up Conference Templates

The RealPresence Resource Manager system uses conference templates and global conference settings to manage system and conference behavior.

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

For more information, see Understanding Conference Templates and Settings on page 389.

Set Up Directory Services

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

To set up RealPresence Resource Manager system directory services, complete the following tasks:

1. Register devices.

   ➢ On endpoints, you can:

   - Set the Global Directory Server (GDS) to point to the RealPresence Resource Manager system IP address or DNS name. We recommend using the IP address to prevent data inconsistencies.
   - Register them to the Polycom DMA system gatekeeper (when it is integrated with your RealPresence Resource Manager system).

   Most device information is automatically populated in the RealPresence Resource Manager system through the gatekeeper registration to an integrated DMA system or Global Address Book access. You must review the information for these devices in the RealPresence Resource Manager system **Directory Setup** page and fill in missing information.

   To select endpoints 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 Understanding Endpoint Management on page 81.

2. Set up users and associate them with endpoints. Unless your RealPresence Resource Manager system is integrated with an enterprise directory, you must enter all user information manually including endpoint association. If your system is integrated with an enterprise directory, general user information (**First Name**, **Last Name**, **UserID**, **Password**, **E-mail Address**) is directly pulled from the directory and cannot be changed. However, you must still associate enterprise users with endpoints. For more information, see Understanding Users, Groups, and Roles on page 278.

3 Set up groups, add members, and associate them with provisioning profiles. For more information, see Understanding Users, Groups, and Roles on page 278.

4 Set up rooms and associate them with endpoints. Unless your RealPresence Resource Manager system is integrated with an enterprise directory that includes conference rooms, you must enter all room information manually including endpoint association. For more information, see Managing Meeting Rooms on page 318.

Set Up a Certificate for the RealPresence Resource Manager System

By default, the RealPresence Resource Manager system uses `https` and a self-signed certificate for its data interchanges. As a best practice, we recommend replacing the RealPresence Resource Manager system self-signed certificate with a certificate from a Certificate Authority. For more information, see Managing Security Certificates on page 346.

Distribute Polycom Applications

The RealPresence Resource Manager system allows you to download several Polycom applications for use in specific environments. This includes two desktop video applications. These are:

- Distribute Polycom CMA Desktop or RealPresence Desktop for Windows Systems
- Distribute Polycom CMA Desktop or RealPresence Desktop for MAC OS Systems

These are discussed in the following topics.

Distribute Polycom CMA Desktop or RealPresence Desktop for Windows Systems

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

To deploy the CMA Desktop or RealPresence Desktop client to users, you have at least four distribution options

Option 1: Distribute the client via an E-mail link

You can copy the link for the client from the RealPresence Resource Manager system **Downloads** page into an E-mail that you can send to users.

To do this, copy and paste the link (for example, `https://10.47.9.170/SoftUpdate/vvl/CMADesktop_5_2_3_19935/CMADesktop.exe`) from the **Downloads** page into an E-mail to be sent to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.

Option 2: Distribute the client via the management system

You can provide users access to the RealPresence Resource Manager system, from which they can download the client.

To do this, copy and paste the IP address of the RealPresence Resource Manager system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the **Downloads** link.

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

Distribute the `.exe` installation file as a desktop management or group policy object to a location on client systems and provide directions to users on how to run the executable.

To do this, build a desktop management or group policy object that writes the `.exe` installation file to a directory (for example, `C:\temp`) on the user’s local system. Include the command for executing the file in an E-mail to be sent to users. For example:

```
C:\temp\CMA Desktop.exe”/s /v"/qn SBSERVERTYPE=2 SBSERVERADDRESS=nnn.nnn.nnn.nnn
```

Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.

Option 4: Distribute the client via a .zip file

Zip the `.exe` installation file and send it in an E-mail to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the e-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the firewall system rather than the RealPresence Resource Manager system. The firewall system should then direct traffic to the RealPresence Resource Manager system.

Option 5: Have users download the client from the Polycom support page

You can tell users to download the client from the Polycom support page (http://support.polycom.com/PolycomService/support/us/support/video/index.html)

User can select a Polycom endpoint (CMA Desktop, RealPresence Desktop, etc) to download.

With this option, you also need to E-mail users the IP address of the RealPresence Resource Manager and the requires username and password.

Distribute Polycom CMA Desktop or RealPresence Desktop for MAC OS Systems

- On a MAC system, the user installing the client must sign in with administrative privileges and an **Administrator** account.
- The following procedures assumes you have implemented DNS lookup and MAC authentication for single signon

To deploy the client for MAC OS clients to users, you have these distribution options:

Option 1: Have users download the client from the Polycom support page

You can tell users to download the client from the Polycom support page (http://support.polycom.com/PolycomService/support/us/support/video/index.html)

User can select a Polycom endpoint (CMA Desktop, RealPresence Desktop, etc) to download.

With this option, you also need to E-mail users the IP address of the RealPresence Resource Manager and the requires username and password.

Option 2: Distribute the Client for MAC OS client via an E-mail link

You can copy the link for the client for MAC OS clients from the RealPresence Resource Manager system **Downloads** page into an E-mail that you can send to users. To do this, copy and paste the client for MAC OS link (e.g., `http://10.47.9.136/SoftUpdate/vvl/CMADesktopMac_5_2_3/CMADesktop.dmg`) from the **Downloads** page into an E-mail to be sent to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users.

Option 3: Distribute the Mac client via the management system

You can provide users access to the RealPresence Resource Manager system, from which they can download the client. To do this, copy and paste the IP address of the client system into an E-mail to be sent to users. Include usernames and passwords (as required) in the E-mail to users and instruct them to access the Downloads link.

Option 4: Distribute the Mac client via a .dmg file

Send the `.dmg` file in an E-mail to users. Include the IP address of the RealPresence Resource Manager system and usernames and passwords (as required) in the E-mail to users. For endpoints on the public network that will be accessing the system through a firewall, include the IP address of the firewall system rather than the RealPresence Resource Manager system. The firewall system should then direct traffic to the RealPresence Resource Manager system.

Conference Scheduling

This section provides an introduction to the Polycom® RealPresence® Resource Manager system video conference scheduling functionality and operations. It includes:

Conference Scheduling Overview

This chapter provides an introduction to the Polycom® RealPresence® Resource Manager system video conference scheduling functionality and operations. It includes:

- Scheduling Participants and Endpoints
- Scheduler Roles
- Conference Types
- Scheduler Overview
- Conference Menu Overview
- User Menu Overview

Scheduling Participants and Endpoints

When you schedule conferences, you select the participants you wish to join the conference from your user directory. Depending on your system configuration, your user directory may be the enterprise directory, the Global Address Book, or one or more local address books. It may also include Guest Book entries.

For participants that have multiple endpoints registered with the RealPresence Resource Manager system, the system selects the participant's default endpoint. You can change to another endpoint by selecting it from the **Call Info** list or by editing the participant.

You can schedule participants without endpoints into conferences. You cannot schedule endpoints without owners into conferences. The RealPresence Resource Manager system can be configured to allow you to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into multiple conferences during the same time period, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences at one time.

Also, if you schedule participants into conference as **Dial In** participants, the conference will require external MCU resources.

Scheduler Roles

Using the RealPresence Resource Manager system web scheduling interface, users assigned the default **Scheduler** and **Advanced Scheduler** roles can create one-time or recurring conferences in a manner similar to other calendar applications.

In the **Scheduler** role, you can schedule conferences and view information about your ongoing, past, and future scheduled conferences. You can also add guests to and delete guests from the system **Guest Book**. You cannot view information for conferences that you did not schedule.

Users assigned the **Advanced Scheduler** role can also select bridges and templates and edit some conference settings.

Role	Supported Actions
View-Only Scheduler	View conferences that other users created
Scheduler	Add a new conference
	Copy a conference you created
	View details of a conference you created
	Delete a conference you created
Advanced Scheduler	Add a new conference
	Specify bridges and select templates for new conferences
	Copy a conference you created
	View details of a conference you created
	Edit some conference settings
	Delete a conference you created
Area Scheduler	Add a new conference
	Edit a future conference you created
	Copy a conference you created
	View details of a conference you created
	Delete a conference you created
Operator	Add a new conference
	Specify bridges and select templates for new conferences
	Copy any conference
	Edit any future conference
	Delete any future conference
	View any conference
	Manage any ongoing conference
	Terminate any ongoing conference

Role	Supported Actions
Area Operator	All area scheduler functions
	All advanced scheduler functions
	Manage any ongoing conference
	Terminate an ongoing conference

Conference Types

This section describes the different types of conferences the system manages. This includes:

- Future and Anytime Conferences
- Direct and Pooled Conferences

Future and Anytime Conferences

When you are scheduling conferences using the RealPresence Resource Manager system, you can add two types of conferences:

- **Future**—Conferences that begin immediately or sometime in the future. These conferences have start and end times and can be recurring. Once you have selected a future conference type, next you decide whether you want to create a Direct Conference or a Pooled Conference.
- **Anytime** — Ad hoc conferences that do not have designated start and end times. These conferences are not recurring. To be able to add Anytime conferences, the RealPresence Resource Manager system must be connected to a Polycom DMA system. For more information, see Schedule an Anytime Conference.

Direct and Pooled Conferences

When first adding a future conference, you can choose between two types of conferences:

- Direct Conference
- Pooled Conference

Direct Conference

A direct conference is a conference that is managed directly on a RMX system through the RealPresence Resource Manager system.

Bridge Selection

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

Because this bridge list depends on the template selection, users should make their template selection before selecting a bridge. Otherwise, they may select a bridge that cannot meet their conferencing requirements. In this case, the conference will fail to schedule.

Those without the Advanced Scheduler role do not see the bridge selection field at all.

Bridge Scheduling and Reassignment

When a conference is scheduled, by default the system automatically assigns the conference to a bridge unless a user with the default **Advanced Scheduler** role intercedes. If that bridge is down at the time the system starts the conference, the RealPresence Resource Manager system attempts to dynamically reassign the conference to another bridge with sufficient capabilities and resources.

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

Some notes about bridge reassignment:

- The bridge reassignment process only occurs when the system detects that a bridge is down. It does not occur if the system determines that a bridge does not have sufficient resources required to host the conference.
- If the RealPresence Resource Manager system cannot find another bridge with the features and capacity needed to support a conference, the conference fails to start. The system does not attempt to modify the conference settings in any way. Instead, the system sends an E-mail to notify the conference organizer of the failure.

The system will chain bridge reassignments. This means that if the next bridge to which the system assigns a conference is down at the time the system tries to start the conference, the system will try to reassign the conference again.

Pooled Conference

A pooled conference is a conference hosted on the Polycom Distributed Media Application™ (DMA) system. Instead of selecting a bridge for your conference, you select a DMA pool order to manage your conference calls.

Pooled conferences are scheduled by the RealPresence Resource Manager system. Resources are allocated at the time of conference initiation by the DMA placing the call on a pool of managed MCUs (RMX or Codian). Using DMA defined priorities, the DMA can manage resource allocation between RealPresence Resource Manager system scheduled conferences and the DMA-initiated ad hoc calls in real-time.

Room ID Numbers

When you create a pooled conference, you can also create a room ID and dial-in number for participants to use. If you don’t specify a room ID, the DMA system will create one and associate it with the scheduled conference.

You can’t use an existing VMR number as the room ID. VMRs that are previously created on the DMA system cannot be used in scheduled pooled conferences.

> You cannot include ISDN endpoints in a pooled conferences. ISDN endpoints are not supported for pooled conferences.

Scheduler Overview

As a scheduler, when you log into the RealPresence Resource Manager system, the system displays the main screen with a **Conference** menu. When you click Conference, you can select from these conference types: Future, Ongoing, or Anytime.

For more information, see Conference Menu and Views on page 44.

> Anytime conferences are supported if the RealPresence Resource Manager system is connected to a Polycom DMA system.

The User menu allows you to select Guest Book and view users or add guests to the guest directory. For more information, see User Menu and Guest Book on page 49.

You might also see these menu items:

Description
Settings. Click here to display a **Settings** dialog box with the following information: • **User Name** • **Remote Server** • **Software Version** • **Font Size** In this dialog box, you can also: • Change the font size used in your display of the RealPresence Resource Manager system web interface. • Change your password, if you are a local system user.
Downloads. Click here to display the **Downloads** dialog box with the downloadable applications compatible with the RealPresence Resource Manager system. Downloadable applications may include: • Polycom CMA Desktop PC or MAC client (including the path to the application) • RealPresence Mobile and Desktop clients • Polycom File Verification Utility
Log Out. Click here to log out of the RealPresence Resource Manager system. **Note** The RealPresence Resource Manager system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time, the system automatically logs you out.
Help. Links to the RealPresence Resource Manager system online help.

Conference Menu Overview

This section includes some general information you should know about the Conference menu and views. It includes these topics:

- Conference Menu and Views
- Conference Views—Future and Ongoing
- Conference Views —Anytime
- Context-Sensitive Conference Actions

Conference Menu and Views

The **Conference** menu provides these views of the **Conference** list:

- **Future**—Displays the list of future scheduled conferences in the main window. Use this view to view and edit future conferences. After selection, the Future-Only filter is enabled.
- **Ongoing**—Displays the list of active scheduled and Anytime conferences in the main window. Use this view to manage ongoing conferences. After selection, the Ongoing-Plus filter is enabled.
- **Anytime** — Displays the list of anytime conferences in the main window.
  Use this view to manage anytime conferences. Anytime conferences are ad hoc conferences that require no start and stop times.

Users can only work with the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list. Operators see all the conferences on the system. However, when areas are defined, operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

The **Future** and **Ongoing** Conference views have these sections.

Section	Description
Views	The views you can access from the page.
Conference Actions	The set of available commands. The constant commands in the **Conference** views are: • **Refresh** — Use this command to update the system display with current information. • **Add** — Use this command to schedule a new video or audio conference. For the list of context-sensitive Conference commands, see Context-Sensitive Conference Actions on page 48.
Conference List	The context-sensitive **Conference** list for the selected view.
Conference Details	Displays information about the selected conference. For more information, see Conference Details on page 78.
Conference Features	Displays the status of system features for the selected conference. For more information, see Conference Features on page 81.

Section	Description
Participants	Displays the list of participants for the selected conference. For more information, see Participants on page 83.
Participant Details	Displays information about the participant selected in the **Participants** list. For more information, see Participant Details on page 83.

Conference Views—Future and Ongoing

The **Conference** list in both the **Future** and **Ongoing** views includes these fields.

Field	Description
Filter	Use the filter to display other views of the conference list, which include: • **Future Only** - Displays scheduled conferences that have not yet started • **Today Only** - Displays scheduled conferences (completed, active, or future) for the current day. • **Custom Date** - Displays scheduled conferences (completed, active, or future) for a selected day. Select the day from the calendar. • **Ongoing Plus** - Displays active and future scheduled conferences for the day. You can further filter this request by **Conference Name**, **Endpoint Name**, **Bridge**, and **Area**. • **Today Plus** - Displays scheduled conferences (completed, active, or future) for the current day, and all future conferences. You can further filter this request by **Conference Name**, **Endpoint Name**, **Bridge**, and **Area**. • **Yesterday Plus** - Displays completed scheduled conferences for yesterday and earlier. You can further filter this request by **Conference Name** or **Area**. These filters apply to scheduled conferences only. Ad hoc conferences are not displayed in the filtered list. For information on filters, see "Filter and Search a List".
Export as Excel file	Click this button to download the currently displayed **Conference** list to a Microsoft Excel spreadsheet.
Status	The state of the conference. For more information, see Conference States on page 47.
Type	The type of scheduled conference. Possible values include: • **Video Conference** — All conference participants have video endpoints. • Direct Conference — Direct conferences are hosted on resources managed by the RealPresence Resource Manager system. • Pooled Conference — Pooled conferences are hosted on resources managed by the Polycom DMA system. • **Audio Only Conference** — All conference participants have audio endpoints. Audio only conferences require an MCU. • **Recurring Conference** ⟳ — The conference is one in a recurring series.

Field	Description
Conference Name	The system- or scheduler-assigned name of the conference. By default, the system assigns a conference name and appends the day and date to that name. The scheduler can change the system-assigned name.
Start Time	The local time of the user’s system for the start of the conference. The system appends the time difference between the local time and the standard time.
Bridge	If applicable, the user-assigned bridge for the conference. Possible values are: • **N/A**—A bridge is not required for this conference • [Bridge Name]—The name of the bridge for the conference. • [Pool Order Name]—The name of the pool order for the conference (pooled conferences only).
Creator	The conference creator.
Area	Area or areas assigned to the selected conference owner. You can only view area-specific information for areas that you have permission to manage. **Note** This field is only visible when Areas are enabled. Your administrator may have renamed this field.
Billing code	Billing code is listed if areas are enabled and billing codes have been assigned to the area. If areas are enabled and a billing code is not assigned, the value is None.

Conference Views —Anytime

> Anytime conferences are supported if the RealPresence Resource Manager system is connected to a Polycom DMA system.

The **Conference** list in Anytime view has these fields.

Section	Description
Title	Name of the conference
Description	Description of the conference
Virtual Meeting Room (VMR)	Virtual meeting room assigned to the conference
Owner	Person who is assigned control of the conference
Created On	Date on the local system when the conference was originally added
# Participants	Number of participants in the conference

Conference States

Conferences may be in the following states.

State	Description
Future Conference	Scheduled conference that has not yet started. This conference state is possible in all views except the **Yesterday Plus** view.
Completed Conference	A scheduled conference that occurred in the past. This conference state is possible in all views except the **Future** and **Ongoing Plus** view.
Active Conference	A conference that is still active/ongoing. This conference state is possible in all views except the **Future** and **Yesterday Plus** view.
Active Alerts Conference	The bridge on which the active/ongoing conference is being hosted has sent an alert. Examples of events that will trigger a bridge alert are: • A participant is connected in secondary mode (audio only). • A conference is not yet full (for example, not all scheduled participants have joined the conference). **Note** This state applies to Direct Conferences only.
Conference End Warning	The conference is ending. For example, the conference is in its last five minutes unless someone extends it.

Context-Sensitive Conference Actions

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

Action	Description
Available for future conferences only	
Edit	Use this command to edit a conference that you have added. For more information, see Edit a Conference on page 62.
Available for future and past conferences	
Delete	Use this command to delete a conference that you have added.
Available for future, past, and ongoing conferences	
Copy	Use this command to copy a conference that you have added.

Action	Description
Available for ongoing conferences only	
Manage	**Operators** only. Use this command to display the **Manage Conference** page for the conference selected in the **Conference List**. Use this command to manage participants and endpoints in the selected active conference. For more information, see Manage an Active Conference on page 66.
Terminate	**Operators** only. Ends the selected conference.

User Menu Overview

This section includes some general information you should know about the Conference menu and views. It includes these topics:

- User Menu and Guest Book
- Context-Sensitive Guest Book Actions
- Add a Guest to the System Guest Book
- Edit a Guest in the System Guest Book
- Delete a Guest from the System Guest Book

User Menu and Guest Book

By default, schedulers, operator, and administrators have access to the **User Menu** and **Guest Book**.

The **Guest Book** is a local system directory that includes guest participants who were either:

- Explicitly added to the **Guest Book**.
- Saved to the **Guest Book** while being added as conference participants.

They are referred to as static entries because they are not imported through the dynamically updated enterprise directory or included in the system **Global Address Book**. The **Guest Book** is limited to 500 entries. The **Guest Book** has these fields.

Field	Description
Name	The guest’s first and last name.
Email	The guest’s E-mail address. The system validates the E-mail structure only.
Location	The location of the guest’s endpoint system. This is a free-form entry field that the system does not validate.
Number	(Optional) The ISDN phone number for the user. This number is constructed from the Country code + Area/City code + phone number or entered as the modified dial number.
Join Mode	Indicates whether the guest will use an audio endpoint or video endpoint to join conferences.

Field	Description
Dial Options	Indicates whether the guest will dial into conferences or that the system should dial out to the guest.
Dial Type	Indicates whether the guest has an H.323 (IP), SIP (IP), or H.320 (ISDN) endpoint.

Context-Sensitive Guest Book Actions

The **Actions** section of the **Guest Book** page may include these context-sensitive actions depending on what is selected.

Actions	Description
Add Guest	Use this command to add a new guest user.
Edit Guest	Use this command to change information for a guest user.
Delete Guest	Use this command to delete a guest from the **Guest Book**. Deleting a guest is a permanent operation.

Add a Guest to the System Guest Book

To add a guest to the system Guest Book

1. Go to **User > Guest Book** and click **Add Guest**.
2. Configure the **Guest Information** section of the **Add New Guest** dialog box.

Field	Description
First Name	The guest’s first name.
Last Name	The guest’s last name.
Email	The guest’s E-mail address. The system only validates the structure of the E-mail address.
Location	The location of the guest’s endpoint system. This is a free-form field that the system does not validate.
Dial Type	Specify the protocol that the guest’s endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the **Add New Guest** dialog box you will need to complete.

Field	Description
Join Mode	Specify whether the guest's endpoint is an audio or video endpoint. **Note** A guest may have multiple endpoints. Create a separate **Guest Book** entry for each endpoint.
Dial Options	Specify whether the guest will dial into conferences, or require that the system dial out to the guest. **Note** To support both options, create a separate **Guest Book** entry for each.

3 If the guest has an H.323 (IP) endpoint, configure these settings:

Field	Description
Number Type and Number	The format and value of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O.
Extension	The specific dial string for the guest. For Annex-O dialing, enter the H.323.alias@IP here, for example: • 1001@11.12.13.14 • 1001@*domain.com* • *username@domain.com* • *username*@11.12.13.14 **Note** Polycom endpoints must register with a gatekeeper before they'll attempt an Annex-O call.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

4 If the guest has a SIP (IP) endpoint, configure these settings:

Field	Description
Sip URI	The SPI URI the MCU must resolve to contact the guest.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

5 If the guest has an H.320 (ISDN) endpoint, configure these settings:

Field	Description
Use Modified Dial Number	Select this option first (as needed) as it will determine the other fields you must configure.
Country	(Not available when **Use Modified Dial Number** is selected.) The country to which the system will dial out to the guest. Click **Select** to view a list of country codes.
Area/City Code	(Not available when **Use Modified Dial Number** is selected.) The area code to which the system will dial out to the guest.
Number	The participant's phone number.
Extension	Cannot be configured.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system has registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

6 Click **OK**.

Edit a Guest in the System Guest Book

To edit a guest in the system Guest Book

1 Go to **User > Guest Book** and select the guest of interest.

2 Click **Edit Guest**.

3 Change the **Guest Information** section and endpoint information sections of the **Add New Guest** dialog box, as needed. For more information about these fields, see Add a Guest to the System Guest Book on page 50.

4 Click **OK**.

Delete a Guest from the System Guest Book

To delete a guest from the system Guest Book

1 Go to **User > Guest Book** and select the guest of interest.

2 Click **Delete Guest**.

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

Conference Scheduling

This chapter describes the Polycom® RealPresence® Resource Manager system conference scheduling operations. It includes these topics:

- Schedule a Future Conference on page 53
- Schedule an Anytime Conference on page 60
- Edit a Conference on page 62
- Edit a Participant’s Settings on page 63
- View Scheduling Information for a Conference on page 64

> Since Area Schedulers can perform both basic and advanced tasks, any references in this chapter to the Scheduler role also applies to the Area Scheduler role.

Schedule a Future Conference

Users with the following default user roles are allowed to schedule Future conferences: scheduler, operator, area operator and area scheduler. The workflow for scheduling a conference includes:

See Conference Scheduling Overview on page 39 for an overview about conference scheduling.

Task Overview

- ➢ Task 1: Set a Time for the Conference on page 54
- ➢ Task 2: Select a Conference Type on page 54
- ➢ Task 3: Select a Bridge or Pool Order to Use on page 55
- ➢ Task 4: Edit Conference Settings on page 56
- ➢ Task 5: Add Conference Participants and Guests on page 59
- ➢ Task 6: Define a Video Chairperson, Lecturer or Owner on page 60
- ➢ Task 7: Review the Conference on page 60

> When scheduling conferences, be aware that the time displayed in the lower left hand corner of the RealPresence Resource Manager system is associated with the time clock of the local PC.
>
> To view the RealPresence Resource Manager system time, navigate to Admin > Server Settings > System Time. You must have the administrator role to view this setting.

Task 1: Set a Time for the Conference

1 Go to **Conference > Future** and under **Conference Actions**, click **Add**.

2 On the conference scheduling page, select either **Direct Conference** or **Pooled Conference**.

> If your RealPresence Resource Manager system is not integrated with a DMA system, you cannot create a Pooled conference.

- Direct Conference - A conference hosted on an MCU that is managed by the RealPresence Resource Manager system. For more information, see Direct and Pooled Conferences on page 41.
- Pooled Conference - A conference hosted on an MCU that is managed by the DMA system. For more information, see Direct and Pooled Conferences on page 41.

3 Enter a new **Conference Name** or accept the default name.

4 Under the **Select Conference Dates and Settings** section, set a conference **Start Date** and **Start Time**, and either an **End Time** or **Duration**.

5 If you want to make the conference recurring:

a Click **Recurrence** and in the Appointment Recurrence dialog box, set:

- Recurrence frequency (Daily, Weekly, or Monthly)
- Recurrence day (Sunday through Saturday)
- Recurrence range (Start date and End After occurrences or End by date)

The maximum number of recurrences is 365.

b Click **OK**.

Task 2: Select a Conference Type

When you are scheduling a direct conference, you need to choose the type of conference you are scheduling. You can schedule a video conference or an audio only conference.

Video conferences can include audio participants. If you choose an audio-only conference, video participants can only participate on audio channels only and no video will be displayed.

6 For **Conference Type**, select **Video** or **Audio Only**.

Task 3: Select a Bridge or Pool Order to Use

Users with the advanced scheduler or operator role can choose a particular bridge or DMA pool order to use for the scheduled conference.

7 If scheduling a direct conference, make your selection from the **Bridge Selection** drop-down list.

- **Auto Bridge**: Allows the system to select a bridge.
- **Single Bridge**: Allows you to select an MCU from the **Scheduled MCU** list to host the conference.

8 If scheduling a pooled conference, make your selection from the **DMA Pool Orders** drop-down list.

9 Select the **Conference Mode** to use.

Conference Mode	Definition
All	Supports all conference modes.
VSW (Video Switching)	Enables a special conferencing mode that provides HD video while using MCU resources more efficiently. All participants see the current speaker full screen (the current speaker sees the previous speaker). If this mode is enabled: • The minimum line rate available is 768 kbps (except for SD resolution, available only on v7 and newer Polycom MCUs with MPM+ or MPMx cards). • All endpoints must connect at the same line rate, and those that don’t support the specified line rate are connected in voice-only mode. • The video clarity, layout, and skins settings are not available. • LPR is automatically turned off, but can be turned back on.
CP (Continuous Presence)	Continuous Presence (CP) mode, in which the MCU selects the best video protocol, resolution, and frame rate for each endpoint according to its capabilities. Select this mode if scheduling only AVC endpoints. This is the only mode that supports the use of Polycom MCU profiles, third-party and legacy endpoints, and legacy RMX MCUs.
SVC (Scalable Video Coding) only	SVC conferencing is only possible with Polycom MCUs and endpoints that support H.264 SVC.
CP and SVC	Enables both AVC-only endpoints and endpoints supporting SVC to join the conference. If the selected MCU doesn’t support SVC, the conference is started in AVC mode. Note: If the MCU supports SVC but not mixed mode (RMX 7.8), the conference fails to start.

10 To change the **Conference Template**, choose a difference template from the **Conference Template** drop-down list.

The available conference templates are automatically filtered according to the **Conference Mode** you selected.

Task 4: Edit Conference Settings

By default, users with the **Advanced Scheduler** role can overwrite certain conference template settings as described here.

Conference settings are view-only unless you have the advanced scheduler role. Users with the advanced schedule role can edit conference settings such as video chairperson, virtual room number, and conference passcode.

Two conferences scheduled with the same template may have different settings and behavior if they are hosted on different types of MCUs. Minimize or eliminate such differences by ensuring that all MCUs are similarly configured.

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

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

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

Setting	Description
Conference ID	By default, the system assigns a **Conference ID**. You can change this ID to permit integration with third-party scheduling tools. This identifier must be 8 or less numeric digits. Note that the RealPresence Resource Manager system compares the **Conference ID** to it's database to verify that it is unique. If it is not unique, you will be prompted to enter a new **Conference ID.**
Conference Passcode	By default, the system assigns an 15-digit **Conference Passcode** and provides this passcode to participants within the content of the conference notification E-mail. You can change this passcode to another 4-digit through 16-digit number.
Enable Chairperson	You can select a video chairperson to control the conference from his or her video endpoint system. The video chairperson must have a video endpoint system and Chairperson conferences require an MCU. **Notes** • If the conference template has the **Conference Requires Chairperson** parameter enabled, then **Enable Chairperson** is automatically selected and cannot be changed. • Polycom RMX 1000 systems do not support the **Chairperson** feature.

Setting	Description
Chairperson Passcode	If **Enable Chairperson** is selected, the system assigns an 15-digit **Chairperson Password** and provides this password to the video chairperson in a separate E-mail. If **Enable Chairperson** is selected, the chairperson must enter this 15-digit password at his or her video endpoint to assume control of the conference. You can change this password to another 4- through 16-digit number.
Virtual Meeting Room Number	Define the virtual meeting room number to be used for this conference. This setting is only available for pooled conferences.
Dial Options	You have three options: • To create a conference for which the same dial-in information and a PIN code are assigned to all conference participants, use the **Dial-In** setting. This setting allows participants to dial in from an audio or video endpoint and connect to the same conference on the MCU. • To dial out to all participants in the conference, use the **Dial-Out** setting. • To allow participants both options, select **Dial-In+Dial-Out**. **Note** When you change a conference from **Dial-In** to **Dial In+Dial Out**, the selected resources remain set to **Dial-In**. You must change them manually.
Always Use MCU	Forces the conference to an MCU and prevents video endpoints from connecting to each other directly. This setting is automatically selected and cannot be changed when Audio Only is the conference type or when **Enable Chairperson** is selected.
Video Mode	Determines the initial layout on a video endpoint's monitor for a multipoint conference that requires an MCU. The options are: • Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. • Select a **Frame Count**, then select the specific layout for the frames. Available layouts are Continuous Presence settings.
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 system reduces the speed that endpoint; however, the conference uses the default connection speed for endpoints that can match it. If you place the calls through an endpoint with an embedded MCU, the behavior depends on the capabilities of that endpoint. 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 conference. Because higher speeds use greater bandwidth, scheduling a high-bandwidth conference may limit the number of conferences that you can reserve at one time.

Setting	Description
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 them on separate screens or through 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 (H.329).** 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. The MCU requires that conferences with People + Content use a minimum speed of 192 K. • **People and Content VO.** This Polycom proprietary technology works with PictureTel endpoints. Select this option for older 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.
T.120 Mode	For MGC-hosted conferences only, selects the protocols and specifications for multipoint data communication. In the **T.120** menu, select the speed for the T.120 connection. See your IT department to determine the best combinations for your conferences. To disable the T.120 mode, select None. If you select T.120, these options may be available, according to the participant’s endpoint and software: • Application Sharing. Allows two or more participants to work on the same document or application, even when only one participant has the application. In application sharing, one participant launches the application, and it runs simultaneously on all other computers. • File Transfer. Enables participants to send files to each other. • Chat or Whiteboard. Allows participants to communicate with each other by writing. In all of these modes, participants can view and hear each other.

13 Once you are satisfied with the conference settings, click **Schedule Conference.**

> - Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.
> - The **Default Template** and **Default Audio Template** are available to all users who can schedule conferences. Other templates may also be available if they have been assigned to users with your role.
> - The **Default Template** and **Default Audio Template** are stored in the system database and their names are not localized.
> - Conference templates for Direct Conferences are defined in the RealPresence Resource Manager system, while conference templates for Pooled Conferences are defined in the DMA system.

Task 5: Add Conference Participants and Guests

14 You may add participants to conferences in the following ways:

➢ To Add Conference Participants from a Directory

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

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

> The search results only include participants associated with endpoints.

b Select the participant of interest's name from the list.

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

c Repeat these steps to add all directory participants and then click **Close**.

➢ To Add Conference Participants from a Guest Book

d Click **Add from Guest Book**.

e In the **Add from Guest Book** dialog box, select the guest of interest's name from the list.

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

f Repeat to add all participants from the **Guest Book** and then click **Close**.

> You must be an Advanced Scheduler to add a guest that is not in the guest book.

➢ To Add New Guest Participants

If you have the advanced scheduler role, you can add new guests to the Guest Book, see Add a Guest to the System Guest Book.

ISDN endpoints cannot participate in pooled conferences.

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

➢ To Add Conference Rooms to a Conference

g Click **Select Site**.

h Select the site of interest from the site list

i The conference room list for the selected site appears.

j Select the conference room of interest from the list.

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

k Repeat these steps to add all required conference rooms and then click **OK**.

Task 6: Define a Video Chairperson, Lecturer or Owner

15 If available, select a **Lecturer**, **Video Chairperson**, or **Owner**.

Task 7: Review the Conference

16 Review your participant list and your settings.

17 Adjust the conference date and time as needed to match participant and endpoint availability. Review availability and adjust the conference date and time as needed.

- For participants who are associated with endpoints, the RealPresence Resource Manager system schedules their availability according to the endpoint's availability.
- For participants with multiple endpoints, check the availability for each endpoint. Click **Call Info** to change the participant's endpoint.
- Dial-in participants can be scheduled to dial into multiple conferences during the same time period; dial-out participants cannot.

To edit a participant's dial settings, select the participant from the **Selected Participants and Rooms** list and click **Edit**. For more information on editing participants settings, see Edit a Participant's Settings on page 63.

Schedule the Conference

18 Click **Schedule Conference** at the top of the page.

Schedule an Anytime Conference

Users with the following default user roles are allowed to schedule Anytime conferences: Scheduler, Advanced Scheduler, Operator, Area Operator and Area Scheduler.

If your RealPresence Resource Manager system is not integrated with a DMA system, you cannot create an Anytime conference.

Unlike Future conferences, Anytime conferences do not have designated start and end times. Once an Anytime conference is configured, conferences can be started at any time by authorized participants. The following events occur when a new Anytime conference is added:

- A participant with scheduling permissions creates a new Anytime conference and the conference is assigned a virtual meeting room (VMR) number.
- The Owner passcode is automatically generated and required to launch an Anytime conference.
- All Anytime conference participants receive an E-mail indicating the VMR number. The owner will also receive the owner passcode needed to launch the conference.
- When a participant dials the VMR number and enters the owner passcode, all dial-out participants are automatically called. If a participant dials into the VMR, they are allowed into the conference or placed on hold until someone dials in and enters the owner passcode.
- The conference continues until all participants hang up the call.

To schedule a new Anytime conference

1. Go to **Conference** > **Anytime** and under Conference Actions, click **Add**.
2. Enter a new conference **Name** or accept the system-generated name.
3. Enter a **Description** for the conference.
4. At **Template**, select a template that your administrator has suggested you use for Anytime conferences.
5. Under **Search for Participants and Rooms**, do one of the following to add a participant or a guest:
   - **To add a participant**: Enter a last and first name and click **Add Participants.** Scroll through the list and click once to add a participant. When finished, click **Close**.
   - **To add a guest**: Enter a last and first name and click **Add from Guest Book**. Scroll through the list and click once on a name in the list. When finished, click **Close**.
6. Select an **Owner** for the conference.
7. Enter a **Virtual Meeting Room ID** to use.
8. To save the conference details, click **Save**.

Copy an Existing Conference

Future and past conferences can be copied as a template for a future conference.

Users can only copy conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To copy a conference

1 Go to the appropriate conference view.

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

3 If you used a template other than the default when you created the conference, re-select the template.

4 Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see Schedule a Future Conference on page 53.

5 When finished, click **Schedule Conference**.

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

6 To exit without sending an updated E-mail message to your participants, click **Skip Email**.

Edit a Conference

You can modify scheduled conferences.

Users can only edit the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Future Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To edit a Future conference

1 Go to **Conference > Future**.

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

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

The conference scheduling page appears.

4 To change the template, click **Default Template** or **Default Audio Template** and select a different template, if available.

- Direct Conference templates provide default conference settings. When you select a different template, you are selecting the default conference settings for your conference.
- The **Default Template** and **Default Audio Template** are available to all users who can schedule conferences. Other templates may also be available to you if they have been assigned to users with your role.
- The **Default Template** and **Default Audio Template** are stored in the system database and their names are not localized.

5 Make the required changes to the conference date, participants, rooms, or other settings. For information on performing these tasks, see Schedule a Future Conference on page 53.

6 When finished, click **Schedule**.

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

7 To exit without sending an updated E-mail message to your participants, click **Skip Email**.

8 To send an updated E-mail to your participants, copy additional people on the notification and/or add notes about the conference.

Note that the **To**, **CC**, and **BCC** fields are ASCII only.

9 Click **Send**.

The system sends the updated conference notification E-mail message. The **Future** view appears. Your conference appears in the conference list.

Edit a Participant’s Settings

You can edit conference participant settings after you have added them to a scheduled conference. If the conference is ongoing or already taken place, you can no longer edit the settings.

When you edit a participant’s settings, those settings are valid only for the current conference that you are scheduling.

Users can only work with the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. In which case operators see all the conferences for the areas to which they belong. By default users assigned other roles cannot view conferences.

To edit a participant’s settings

1 Go to **Conference > Future**.

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

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

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

5 In the Edit Participant Settings dialog box, you can edit the participant settings as required:

Field	Description
Endpoints	Select an endpoint from the list.
Dial Options	Select either Dial-In or Dial-Out.
Dial Type	Select either H.323, SIP (SIP URI) or H.320. If no dial type is selected, it defaults to E.164.

6 When finished, click OK.

View Scheduling Information for a Conference

Users can only view scheduling information for the conferences that appear in their **Conference** list. By default, schedulers see only their conferences in the **Conference** list, while operators see all the conferences on the system, unless areas are defined. When areas are defined, operators see all the conferences for the areas to which they belong. By default, users assigned other roles cannot view conferences.

To view the scheduling information for a Future or Ongoing conference

1 To see the scheduling information for a future conference, go to **Conference > Future**. To see the scheduling information for an active conference, go to **Conference > Ongoing**.

2 From the **Filter** list, select the conference type of interest.

3 Select the conference to view from the list. Under **Conference Actions**, click **View.**

The **View** conference page appears displaying the following details about the selected Future or Ongoing conference:

Section	Description
Conference Name	The system- or scheduler-assigned name of the conference. By default, the system assigns a conference name and appends the day and date to that name.
Start Date	The date on which the conference started or will start.
End Date	The date on which the conference is scheduled to end.
Duration	The scheduled duration of the conference in hours and minutes.
Recurrence	The recurrence information for the conference.
Owner	The designated person in control of the conference.
Type	The type of conference, either Audio-Video or Audio only.

Section	Description
Conference Passcode	View only. The conference passcode assigned to the conference. For Future conferences, users with the **Advanced Scheduler** role can change this conference password.
Video Chairperson	Whether or not the conference has a video chairperson. This field will include a participant's name or No Chair. For Future conferences, users with the **Advanced Scheduler** role can assign a conference chairperson.
Conference Area	The area to which the conference owner belongs. **Note: This field is only visible when Areas are enabled.** You can only view area-specific information for areas that you have permission to manage.
Participants	Information about the conference participants, including • Name • Dial Mode • Participant Type • Access • Endpoint • Area

4 To return to the conference list, click **Back to List**. You might need to scroll down to see the **Back to List** button.

To view the scheduling information for an Anytime conference

1 To see scheduling information for an Anytime conference, click Conference > Anytime or under Views, click **Anytime**.

The list of anytime conferences is displayed.

2 To view details about a particular anytime conference, select the conference, then view the Participants pane or click **Edit**.

For descriptions of these details, see Conference Views —Anytime.

3 The following Participant details are displayed:

Field	Description
Name	Name of the participant
Call Info	Call information about the participant, including Video Dial-Out, Video Dial-In, or an IP address
Call Type	Information about the call type, either H.323, SIP (IP), or H.320 (ISDN).
Dial Options	The type of participant call, either Dial-In or Dial-Out.

Managing Conferences and Participants

This chapter describe the Polycom® RealPresence® Resource Manager system conference and participant management operations. It includes these topics:

- Manage an Active Conference
- Add Additional Participants to an Active Conference
- Add a Room to an Active Conference
- View the Video of a Participant in an Active Conference
- Join an Active Conference
- Add a Participant from a Favorites List to an Active Conference
- Add/Save a Participant to a Favorites List
- Manage a Participant's Endpoint During a Conference
- View a Participant's Details During a Conference
- Terminate an Active Conference
- Delete a Conference
- Export a List of Conferences

Manage an Active Conference

The **Manage Conference** page provides a detailed view of a single active conference and allows an operator to make changes to the conference.

> You cannot monitor or manage adhoc conferences taking place on the DMA system. These conferences may display in the ongoing conferences list but because the RealPresence Resource Manager system does not directly manage ad hoc conferences that take place on bridges managed by the DMA system, conference information is inconsistent.

To manage an active conference

1 Go to **Conference > Ongoing**.

2 From the list of **All Conferences**, select the conference of interest and click **Manage**.

The conference page appears in a new tab displaying the **Participants** list. The **Participants** list displays these settings:

Section	Description
Status	The state of the participant's connection as identified by an icon. Hover over the icon to determine the status.
Type	The type of conference as identified by an icon. Hover over the icon to determine the type.
Name	The participant's name.
Endpoint	The name assigned to the participant's endpoint when it registered or was added to the system.
Access	The endpoint's network interface type. Possible values include: • H323 • ISDN • SIP
Address	The IP address, or ISDN number of the participant's endpoint (if a dial-out), or SIP URI.
Bit Rate	The sum of the audio and video data transfer rate (in kbps) of the participant's endpoint.
Dial Mode	How the participant joined the call. Possible values include: • Audio or Video Dial-In • Audio or Video Dial-Out
Bridge	The MCU on which the participants call resides.

3 Use these conference actions as needed:

Action	Use this action to...
Terminate	End an active conference.
Extend Duration	Extend the duration of an active conference.
Change Layout	For applicable endpoints. Change the default video layout for the conference display. • Switching. Indicates that the display changes each time the speaker changes, and everyone sees the current speaker. • Select a **Frame Count**, then select the specific layout for the frames. The available layouts are Continuous Presence settings.
Add Participant	Add one or more participants to the selected conference.
Add Guest	Add a guest to the selected conference.
Add Room	Add one or more rooms to the selected conference.

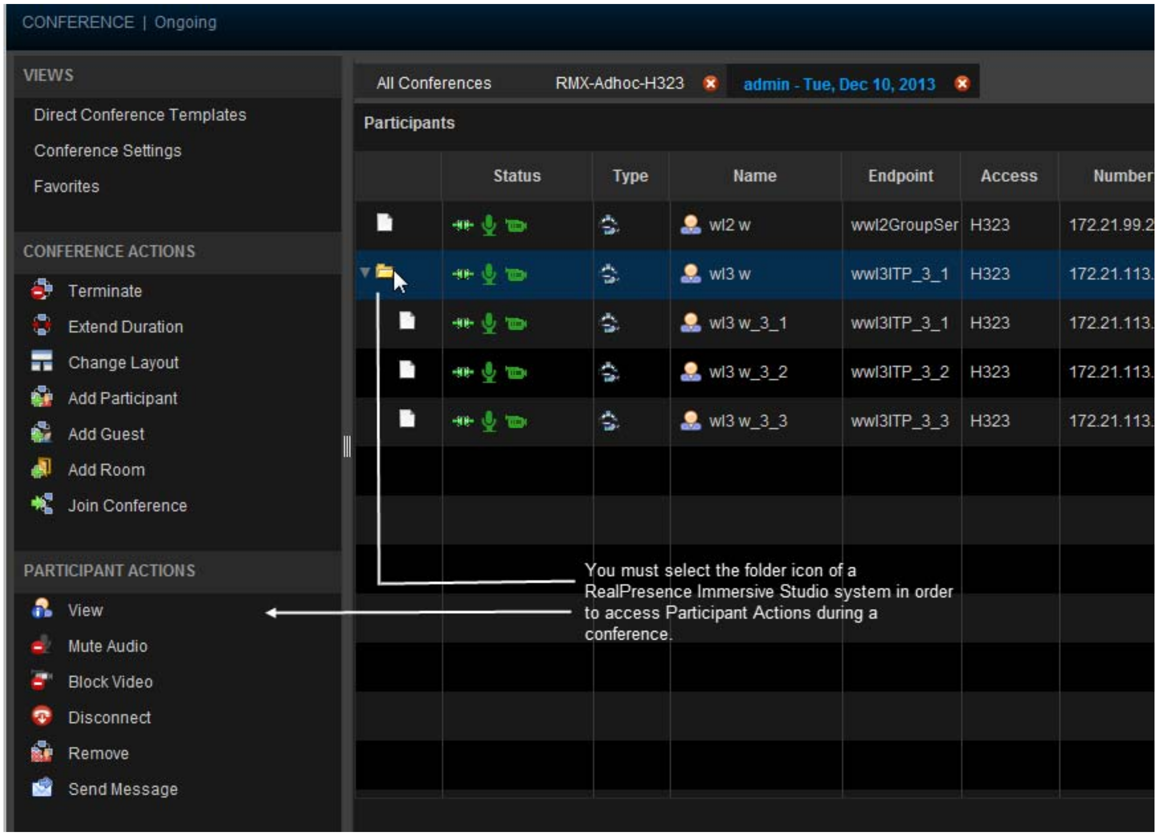
Action	Use this action to...
Add Favorites	Add participants from one of your Favorites lists to the selected conference.
Join Conference	Join the conference, monitor the conference, and talk with participants as needed.

4 Use these participant actions as needed:

Action	Use this action to...
Mute or Unmute Audio	Mute or unmute the selected participant’s audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.
Block or Unblock Video	Block or unblock the selected participant’s video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.
Connect or Disconnect	Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.
Remove	Remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.
Send Message	Send a message to the selected participant’s registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.
Acknowledge Help	Acknowledge a request for help and send a message to the requesting endpoint.
Manage Device	Open the web-based user interface for the selected participant’s endpoint in a new browser window.
Save as Favorite	Function available when the selected participant has an associated endpoint to which the system can dial out. Save the selected participant to an existing Favorites List.
Connect All New	Function available only when the system is displaying the **New Conference Participants** list. Initiates the system dial out to new participants.

Working with RealPresence Immersive Studio Systems

RealPresence Immersive Studio systems display as expandable folders containing an icon for each of the codecs associated with the endpoint. You can only perform **Participant** actions on a RealPresence Immersive Studio system when you have the folder selected.



	Status	Type	Name	Endpoint	Access	Number
			wl2 w	wwl2GroupSer	H323	172.21.99.2
			wl3 w	wwl3ITP_3_1	H323	172.21.113.
			wl3 w_3_1	wwl3ITP_3_1	H323	172.21.113.
			wl3 w_3_2	wwl3ITP_3_2	H323	172.21.113.
			wl3 w_3_3	wwl3ITP_3_3	H323	172.21.113.

You must select the folder icon of a RealPresence Immersive Studio system in order to access Participant Actions during a conference.

Writing Conference Notes During a Conference

Participants with scheduler permissions can write conference notes during an ongoing conference.

To create a conference note

» Click the **Conference Notes** pane, type a note, and click **Save**.

The note becomes visible on any RealPresence Resource Manager browser session where other users are monitoring the same conference.

> If you type a note and then decide to undo your changes, click Escape to return to the original note.

Add Additional Participants to an Active Conference

Users with the Operator role can add additional participants to an active conference.

To add participants from the local directory or enterprise directory

1 Go to **Conference > Ongoing**.

2 From the list of **All Conferences**, select the conference of interest and click **Manage**.

3 Click **Add Participant**.

4 Enter all or part of a participant's **Last Name** or **First Name** into the appropriate field and click **Search**.

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

> The search results only include users associated with endpoints.

5 Select the participant's name from the list.

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

6 Repeat steps Click Add Participant. through Select the participant's name from the list. to add all domain participants and then click **Close**.

7 If necessary, edit the new participants' settings. See Edit a Participant's Settings on page 63.

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

The system dials out to the participants and adds them to the conference.

To add participants from the Guest Book

1 Click **Add Guest**.

2 From the **Guest Book** dialog box, select the guest's name from the list.

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

3 Repeat step From the Guest Book dialog box, select the guest's name from the list. to add all guest participants and then click **Close**.

4 To add new guest participants (participants not available from the local directory, enterprise directory, or **Guest Book**), see step To Add New Guest Participants on page 59.

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

The system dials out to the participants and adds them to the conference.

Add a Room to an Active Conference

To add a room to an active conference

1. Go to **Conference > Ongoing**.
2. From the list of **All Conferences**, select the conference of interest and click **Manage**.
3. From the **Conference Actions** list, click **Add Room**.
4. From the **Add Room** dialog box, select the site location of the room.

   The list of conference rooms at the site appears.
5. Select the conference room of interest.

   The conference room name appears in the underlying **New Conference Participants** list.
6. Click **Close**.
7. To initiate the system dial out to the room, select the room from the **New Conference Participants** list and click **Connect New Participants**.

   The system dials out to the room endpoint system and adds the room to the conference.

View the Video of a Participant in an Active Conference

To view the video of a participant in an active conference

1. Go to **Conference > Ongoing**.
2. From the list of **All Conferences**, select the conference of interest and click **Manage.**
3. Select a participant from the **Participants** list.

   The selected participant’s video appears in the **Conference Image** section of the interface.
4. Click **Shuffle** to shuffle to the next participant’s video.

Join an Active Conference

By default, users assigned the **Operator** role can join an active conference to offer conference support.

To join an active conference

1. Go to **Conference > Ongoing**.
2. From the list of **All Conferences**, select the conference of interest and click **Manage.**
3. From the **Conference Actions** list, click **Join Conference**.

   The **Join Conference** dialog box appears.
4. If you have multiple endpoints, choose the endpoint to use to join the conference.

5 Click **Join Conference**.

Your endpoint is added to conference with your video blocked but your audio not muted.

Add a Participant from a Favorites List to an Active Conference

By default, users assigned the **Operator** role can work with favorites lists.

To add a participant from a favorites list to an active conference

1 Go to **Conference > Ongoing**.

2 From the list of **All Conferences**, select the conference of interest and click **Manage.**

3 From the **Conference Actions** list, click **Add Favorites**.

4 From the **Favorites List**, expand the list of interest.

The names of the participants in the list is displayed.

5 Select the participant of interest from the list.

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

6 Repeat steps From the Favorites List, expand the list of interest. and Select the participant of interest from the list. to add all participants from **Favorite’s List** and then click **Close**.

7 To initiate the system dial out to new participants, select the participants of interest from the **New Conference Participants** list and from the **New Participants Action** menu, click **Connect New Participants**.

The system dials out to the participants and adds them to the conference.

Add/Save a Participant to a Favorites List

By default, users assigned the **Operator** role can work with favorites lists.

To add or save a conference participant to a favorites list

1 Go to **Conference > Ongoing**.

2 From the list of **All Conferences**, select the conference of interest and click **Manage**.

3 From the **Participants** list, select the participant of interest.

4 From the **Participant Actions** menu, click **Save as Favorite**.

The names of the participants in the list is displayed.

5 From the **Save as Favorite Participant** dialog box, select the Favorite List to which to save the participant and click **OK**.

Manage a Participant’s Endpoint During a Conference

The **Manage** page also allows operators to manage conference participant’s endpoints.

- 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 endpoint

1. Go to **Conference > Ongoing**.
2. Select the conference of interest and click **Manage**.

   The **Participants** list appears.
3. To view participants geographically, click 🖼.
4. Double-click on the participant of interest.
5. Use these participant actions as needed. These actions are also available from the **View Participants Details** dialog box.

Action	Use this action to...
Mute or Unmute Audio	Mute or unmute the selected participant’s audio line into the conference. This option appears only when the conference is running on an external MCU. The Audio column in the Participants list shows the current status of this setting.
Block or Unblock Video	Block or unblock the selected participant’s video line into the conference. This option appears only when the conference is running on an external MCU. The Video column in the Participants list shows the current status of this setting.
Connect or Disconnect	Disconnect or reconnect the selected participant to the conference. A disconnected participant is still associated with the conference and cannot be scheduled for other conferences.
Remove	Remove the selected participant from the Participants list at which time the participant can be scheduled for another conference.
Send Message	Send a message to the selected participant’s registered Polycom endpoint. The message appears briefly on the monitor for the selected video endpoint.
Acknowledge Help	Acknowledge a request for help and send a message to the requesting endpoint.
Manage Device	Open the web-based user interface for the selected participant’s endpoint in a new browser window.

Action	Use this action to...
Save as Favorite	Function available when the selected participant has an associated endpoint to which the system can dial out. Save the selected participant to an existing Favorites List.
Connect All New	Function available only when the system is displaying the **New Conference Participants** list. Initiates the system dial out to new participants.

View a Participant’s Details During a Conference

This procedure describes how to view details for a participant’s endpoint while it is in conference.

> **Working with RealPresence Immersive Studio systems**
>
> RealPresence Immersive Studio systems display as expandable folders containing an icon for each of the codecs associated with the endpoint. You can only perform actions on the master codec. The master codec is indicated by name of the codec that ends with “_1”.

To view a participant’s endpoint details

1 Go to **Conference > Ongoing**.

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

The **Participants** list appears.

3 To view participants geographically, click 🗺.

4 Double-click on the participant of interest.

The **View Participant Details** dialog box appears with the **Call Properties** displayed. It includes the **Near End** and **Far End** video, the Participant’s name, **Status**, **Errors**, **Warnings**, **Endpoint** Type, **Address**, **Access**, and **Bit Rate**.

It also includes a list of **Participant Actions**. For more information about these actions, see Manage a Participant’s Endpoint During a Conference on page 73.

5 To view additional participant details, change the selection in the **Call Properties** drop-down menu.

➢ If you select **Device**, you’ll see these participant details:

Setting	Description
Endpoint Type	Usually the endpoint model, such as Polycom HDX system.
IP Address	The IP address for the endpoint.
Site	The location of the endpoint as identified by its IP address and the subnet of the site.

Setting	Description
Gatekeeper	The gatekeeper with which the endpoint is registered.
GDS	The Global Directory Service for the endpoint. Usually the Polycom Global Address Book.
Presence	Whether or not the endpoint is registered with a Presence service, so that its availability can be reported.
Device Managed	Whether or not the endpoint is registered with a Provisioning service, so that it can be configured automatically.
ISDN Line Status	The status of the ISDN line. Possible values include: • Operational • Non-operations This field is blank for the following endpoint types: **PVX**, **MGC**, **RMX**, **GW/MCU**, **Other**, and **TANDBERG**.
Alias Type	If the endpoint has an alias designation, the type of alias. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown.
Alias Value	Value for the alias type shown.

➢ If you select **Call Details**, you'll see these participant details:

Setting	Description
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include: • H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the endpoint is using.
Video Rate	The video bandwidth negotiated with the far site.
Video Rate Used	The actual video bandwidth used in the call to the far site.
Video Frame Rate	Specifies the frame rate to use.
Video FEC Errors	The number of Forward Error Correction (FEC) errors that have been corrected in the current call.
Cause Code	

Setting	Description
Audio Rate	The audio bandwidth negotiated with the far site
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using.

- If you select **Call Quality of Service**, you'll see these standard service measurements: Total Packet Loss, % Packet Loss, Audio Packet Loss, Video Packet Loss, Audio Jitter, and Video Jitter.

Terminate an Active Conference

To terminate an active conference

1. Go to **Conference > Ongoing**.
2. Select the conference of interest and click **Terminate**.
3. Click **Terminate** to confirm the termination.

Delete a Conference

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

To delete a conference

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

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

Export a List of Conferences

Users with the Operator or Admin role can export a list of Future conferences to a CSV file.

This option is only available when the list of conferences is filtered by Future Only.

To export a list of future conferences to a CSV file

1. Navigate to **Conference > Future**.
2. In the **All Conferences** list, be sure the list is filtered according to the **Future Only** filter.
3. Click **Export as CSV File.**

Conference and Participant Details Reference

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

- Conference Image on page 78
- Conference Details on page 78
- Conference Features on page 81
- Bridge (MCU) Features on page 82
- Participants on page 83
- Participant Details on page 83

Conference Image

The **Conference Image** section displays the selected participant's video. Click **Shuffle** to shuffle to the next participant's video.

Conference Details

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

Section	Description
Creator	Name of the person who created the conference. Not applicable for ad hoc conferences.
Owner	Name of the owner of the conference, if an owner is selected. **Note** Not applicable for Anytime conferences.
Start Date/Time	For a scheduled conference, the start date and time of the conference and the time difference between the local time and the standard time. For an unscheduled conference, the date and time the conference started.
Duration	For a scheduled conference, how long the conference is scheduled to last. For a completed conference, how long the conference actually lasted.
End Date/Time	The date and time the conference ended

Section	Description
Type	The type of conference. Possible values include: • Audio • Audio-Video
Status	The state of the conference. Possible values include: • Active Alerts • Declined • Finished • Future
Recurring	Whether or not the conference was scheduled as a recurring conference
Connection	Connection information about the conference. Possible values include: • Multipoint • Point To Point • Gateway • Embedded Multipoint
Bit Rate	The rate (in kbps) at which to transfer the conference audio or video data
Conf Monitoring ID	System-assigned ID used for troubleshooting
Media Type	Describes the media type used for the conference.
Video Session Type	Type of video session: VSW (Video Switching) CP (Continuous Presence) SVC (Scalable Video Coding) only CP and SVC

Section	Description
Video Layout	The video layout for the conference. For more information about layouts, see your MCU documentation. Possible values are: VIDEO_SWITCHING CP_1X1 CP_1X2 CP_2X1 CP_2X2 CP_3X3 CP_1AND5 CP_1AND7 CP_1X2VER CP_1X2HOR CP_1AND2HOR CP_1AND2VER CP_1AND3HOR CP_1AND3VER CP_1AND4VER CP_1AND4HOR CP_1AND8CENTRAL CP_1AND8UPPER CP_1AND2HORUPPER CP_1AND3HORUPPER CP_1AND4HORUPPER CP_1AND8LOWER CP_4X4 CP_2AND8 CP_1AND12 CP_1X1QCIF CP_1X2FLEX CP_1AND2HORRFLEX CP_1AND2HORLFLEX CP_1AND2HORUPPERRFLEX CP_1AND2HORUPPERLFLEX CP_2X2UPPERRFLEX CP_2X2UPPERLFLEX CP_2X2DOWNRFLEX CP_2X2DOWNLFLEX CP_2X2RFLEX CP_2X2LFLEX CP_UNKNOWN
Video Format	For a conference hosted on an MCU, the video format of the conference data stream. Possible values include: • Automatic • CIF • QCIF • 4CIF • 16CIF • VGA • SVGA • XGA • NTSC
Video Protocol	For a conference hosted on an MCU, the video protocol of the conference data stream. Possible values include: • Auto • H.261 • H.263 • H.264
Audio Algorithm	For a conference hosted on an MCU, the audio compression ratio of the conference data stream. Possible values are: • AUTO • G.711 • G.722 • Siren 7 (16 kbps)

Section	Description
Conference Area	Area or areas assigned to the selected conference owner
Participant Areas	List of areas to which participants belong

Conference Features

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

Section	Description
Conference Passcode	The conference passcode, which is assigned either by the system or the scheduler.
Chairperson Option	Indicates whether or not the conference requires a chairperson. **Note** The RMX 1000 system does not support the **Chairperson** feature.
Chairperson Passcode	The passcode the chairperson must enter to take control of the conference. Not applicable when no chairperson is designated.
Chairperson	The name of the chairperson. Not applicable when no chairperson is designated.
Dial-in #	The number that can be used by participant not explicitly invited to the scheduled conference.
Lecture Mode	The type of **Lecture Mode**, if any, that was selected when the conference was created. Possible values are None, Lecture, and Presentation. **Note** The RMX 1000 system does not support **Lecture Mode**.
Lecturer	The name of the lecturer. Not applicable when **Lecture Mode** is **None**.
Lecture View Switching	Indicates whether or not automatic switching between participants is enabled.
Dual Stream Mode	Possible values are: • None • People+Content • Visual Concert PC • Visual Concert FX • Duo Video • Unknown •

Section	Description	
T120 Rate	Possible values are: • None • HMLP - Var • HMLP - 384 • HMLP - 320 • HMLP - 256 • HMLP - 192 • HMLP - 128 • HMLP - 6.4 • HMLP - 62.4 • HMLP - 14.4 • MLP - Var • MLP - 64.4	• MLP - 62.4 • MLP - 46.4 • MLP - 40 • MLP - 38.4 • MLP - 32 • MLP - 30.4 • MLP - 24 • MLP - 22.4 • MLP - 16 • MLP - 14.4 • MLP - 6.4 • MLP - 4
End Time Alert	Whether or not the system alerts participants to the end of the conference by playing an end tone	
Entry Tone	Whether or not an entry tone is played to all connected participants when a participant joins the conference	
Exit Tone	Whether or not an exit tone is played to all connected participants when a participant disconnects from the conference	

Bridge (MCU) Features

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

Section	Description
MCU Name	The MCU device name hosting the conference. Not applicable when the conference is not being hosted on an MCU.
Numeric ID	The unique conference identifier assigned by the MCU
Entry Queue Access	Whether or not the conference has an entry queue enabled **Note** The RealPresence Resource Manager system enables entry queues on a per MGC basis and all conferences on an entry queue enabled MGC will be scheduled with entry queue access.
Meet Me per Conf	Whether or not the a conference is a Meet Me conference, for which a dial-in number is assigned, so that undefined participants can connect to the conference
Conference on Port	(MGC only) Indicates whether or not the MGC is set to Conference on Port, which conserves bandwidth and ports. In this case, all participants are on a single video port and use the same connection speed and video format.

Section	Description
Message Service Type	Displays the type of messages participants joining the conference hear. Possible values are: • None • Welcome (No wait) • Attended (Wait) • IVR
Message Service Name	Name on the MCU of the Message Service. So, for example, a service name IVR70 which provides the IVR service

Participants

On the Future and Anytime screens, the list of participants identifies users, rooms, and guests invited to participate. The list on the Ongoing screen identifies participants actively on a call.

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

Participant Details

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

Section	Description
Name	The participant’s name
Type	The type of conference connection. Possible values include: • Audio Only • Audio-Video • Other (for **In Person** and **Room Only** participants)
Endpoint Name	The name assigned to the participant’s endpoint when added to the system

Section	Description
Connection Status	The state of the participant’s endpoint connection. Possible values include: • Connected • Connecting • Declined • Disconnected • Disconnecting • Error • Unknown
Interface Type	Possible values are: • H323 • ISDN • SIP • H323_E164 • H323_ANNEX_O • H323_ID
Address	Used to reach endpoints, such as IP address or E164 number
Number	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)
Bit Rate	The audio or video data transfer rate (in kbps) of the participant’s endpoint
Encryption	Encryption is either enabled (True) or disabled (False)
Area	Area or areas assigned to the participant.

Endpoint Operations

This section provides an introduction to the Polycom® RealPresence® Resource Manager system endpoint management functionality and operations. It includes:

Managing Endpoints

Supported Endpoint Types

Endpoint Device Details

Managing Endpoints

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system's endpoint operations. It includes these topics:

- Endpoint Management on page 86
- Endpoint Associations and Presence on page 87
- Endpoint Passwords on page 87
- Add and Monitor Endpoints and Peripherals on page 93
- Download an Endpoint Inventory Report on page 105

Endpoint Management

Endpoint management eliminates the need to configure each endpoint individually through the hand-held remote or the endpoint's web interface. It also helps you easily enforce network, group and system policies for each device.

Endpoint management consists of two aspects of remotely configuring endpoints: updating software and provisioning settings.

The RealPresence Resource Manager system allows you to manage endpoints in two ways:

- Scheduled Management of Endpoints (Polycom and Third-Party) on page 86
- Dynamic Management of Endpoints (Polycom Only) on page 86

Scheduled Management of Endpoints (Polycom and Third-Party)

Scheduled management allows you to push software updates and provisioning profiles to endpoints at intervals that you define.

Scheduled management uses server-to-client communication over HTTP. This management technique is more appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.

Dynamic Management of Endpoints (Polycom Only)

Dynamic management allows the endpoint to poll the RealPresence Resource Manager automatically to get provisioning updates (configuration settings) and software updates based on policies you define.

The administrator can use a rule-based system to apply dynamic provisioning profiles. An administrator can create multiple rules and associate a profile with more than one rule at a time. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied.

Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is available:

- Only for Polycom endpoints.
- When Polycom endpoints are able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager system.

In dynamic management mode, when an endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package or provisioning profile. If a either is found, the package is sent in XML format over a secure HTTPS connection.

Endpoints do not poll the system if they are in a call. They restart polling after the call ends.

For more information about dynamic management methods, see Understanding Dynamic Endpoint Management on page 156.

Endpoint Associations and Presence

The RealPresence Resource Manager system assumes that users will be associated with endpoints. You can associate a user with more than one endpoint, but one endpoint is designated as the primary endpoint.

When scheduling a user in a conference, the RealPresence Resource Manager system will, by default, schedule the user’s primary endpoint. The scheduler can choose to change the request to schedule one of the user’s other endpoints.

The RealPresence Resource Manager system is also a presence service, which is the part of the system that maintains online status information for the users of dynamically managed endpoints. The presence service allows users to access information about the online status of other users. This is important, because when you make a video call or start a chat, that action only takes you to a endpoint. It doesn’t ensure that you will reach the person you want to reach. The presence service provides information about the user’s availability, which improves your chances of getting the person.

> The RealPresence Resource Manager supports presence services for all dynamically-managed Polycom endpoints with the exception of RealPresence Mobile.
>
> RealPresence Desktop clients managed by the RealPresence Resource Manager can now received offline messages.

Endpoint Passwords

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

- Schedule provisioning of an endpoint through a RealPresence Resource Manager system.

- Use the Scheduled Software Update feature.
- Monitor the endpoint from the **Endpoint > Monitor View**.

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

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

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

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

Endpoint Menu, Views, and Lists

The RealPresence Resource Manager system **Endpoint** menu provides these views of the **Endpoint** list:

- **Monitor View**—Displays the list of all registered and managed endpoints. Use this view to monitor and manage endpoints.
- **Peripherals View**—Displays the list of all peripherals connected to managed endpoints. Use this view to see the status of peripherals.
- **Dynamic Management**—Displays the list of actions for dynamically managing endpoints eligible.
- **Scheduled Management**—Displays the list of actions for using scheduled endpoint management.

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

Section	Description
Views	The views you can access from the page.
Actions	The set of available commands. The constant command in the **Endpoint** views is **Refresh** , which updates the display with current information.
Endpoint List	The context-sensitive **Endpoint** list for the selected view.
Device Information	Information about the endpoint selected in the endpoint list including: • Endpoint Device Summary Information on page 115 • Device Status Information on page 117 • Call Information on page 118 • Device Alerts Information on page 119 • Provisioning Details on page 119 • Software Update Details on page 120

Monitor View

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

Endpoint List in the Monitor View

By default the Endpoint list in the Monitor View displays a list of all endpoints that are registered with the RealPresence Resource Manager system for management and monitoring purposes. The endpoints are listed in only 50 endpoints at a time and you can page through the list in its entirety.

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

Field	Description
Filter	Use the filter choices to display other views of the **Endpoint** list, which include: • **Type** - Filters the list by type. For more information, see Supported Endpoint Types on page 109. • **Alerts** - Filters the list by alert type: Help, Error, or Warning. • **Connection Status**- Filters the list by connection status: In a Call, Online, or Offline. • **Name** - Filters the list by system name entered. • **IP Address** - Filters the list by IP address entered. • **Dial String**- Filters the list by dial string (SIP, H.323, or ISDN) entered. • **Site** - Filters the list by site location entered. • **Area not the same as Site's Area** - Available only when Areas are enabled. This filters endpoints that belong to a site which is not associated with the area the endpoint belongs to. If the user does not manage the site's area, he cannot view the Site area information. The value for the area will display as "Restricted". • **Area** - Available only when Areas are enabled. Filters the list by the area with which the endpoint is associated. This field is only visible when Areas are enabled. You can only view area-specific information for area(s) that you have permission to manage. • **VIP** - Filters the list for VIP endpoints.
Status	The state of the endpoint. Possible values include: • Online • Offline • Licensed • In a call • Gatekeeper registered • Signalling unregistered • Error • All paired peripherals are connected without alerts • One or more paired peripherals are turned off or no longer connected • One or more paired peripherals has an error

Field	Description
Mode	The management mode for the endpoint. Possible values include: • Dynamic management mode ★ • Scheduled management mode (no icon) For a description of these modes, see Understanding Endpoint Management on page 81.
Name	The assigned name of the endpoint.
Model	The type of endpoint. For valid endpoint types, see Supported Endpoint Types on page 109.
IP Address	The IP address assigned to the endpoint.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.
Dial String	The dial string for the endpoint. If the endpoint has more than one dial string, it displays one based on this order: • SIP • H.323 • ISDN
Site	The site to which the endpoint belongs. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Owner	The user associated with the endpoint.

Actions in the Monitor View

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

Action	Use this action to...
Available for all endpoint types	
View Details	Display all of the **Device Details** for the selected endpoint.
Edit	Change connection settings for the selected endpoint. Note that if this is a managed endpoint, the endpoint may overwrite settings entered manually.
Delete	Delete the selected endpoints.
Search Devices	Search the list of endpoints by IP range.

Action	Use this action to...
Available for only selected endpoint types	
Add	Manually add an endpoint to the RealPresence Resource Manager system or find a endpoint on the network. This command is not available for Polycom endpoints that must be dynamically-managed: **RealPresence Mobile**, **RealPresence Desktop**, **RealPresence Group** systems and **RealPresence Immersive Studio** systems.
Manage	Open the selected endpoint's management interface in a separate browser window. This command is not available for the following endpoint types: **RealPresence Mobile**, **RealPresence Desktop** and **CMA Desktop** systems.
Send Message	Send a text message (ASCII only, 100 characters maximum) to the selected endpoint's video monitor. This command is not available for the following endpoint types: **TANDBERG**, **Other**, **RealPresence Mobile**, **RealPresence Desktop** and **CMA Desktop** systems.
Clear Help	Clear help for the selected endpoint on the RealPresence Resource Manager system.
Reboot Device	Reboot the selected endpoint. This command is only available for **HDX-Series, Group-Series** and **VSX-Series** endpoints with a **Connection Status** of **Online**.
Search Devices	Allows you to search for endpoints within a range of IP addresses. The results message displays the number of endpoints searched and the number of endpoints found within the IP range. This command is not available for the following endpoint types: **RealPresence Mobile**, **RealPresence Desktop**, **RealPresence Group** systems and **RealPresence Immersive Studio** systems.
Manage Owner	Edit information for the user (owner) of the selected endpoint. This command is applicable only when a user is associated with the endpoint.
View Peripherals	View information about peripherals. This command is only available when one or more peripherals is connected to an **HDX-Series** or **Group-Series** endpoint.
Associate User	Manually associate a user with the selected endpoint.
Assign Area	(Available only when Areas are enabled.) Associate the selected endpoint to an area. An endpoint can only be assigned to a user who belongs to the same area as the endpoint. Users can only view area information for the areas to which they have been assigned to manage.

For information about these endpoint actions, see Understanding Endpoint Management on page 81.

Peripherals View

Use the **Peripherals View** to monitor peripherals connected to dynamically managed endpoints.

Peripherals List in the Peripherals View

By default the **Peripherals** list displays a list of all peripherals that are connected or have been connected to endpoints managed by the RealPresence Resource Manager system.

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

Field	Description
Filter	Use the filter choices to display other views of the **Endpoint** list, which include: • **Type** - Filters the list by type. • **Paired Endpoint** - Filters the list by the endpoint to which the peripherals are connected. • **IP Address** - Filters the list by IP address entered. • **Hardware Version** - Filters the list by hardware version entered. • **Software Version** - Filters the list by software version entered.
Status	The state of the peripheral. Possible values include: • Connected ⇆ - Peripheral is connected to the endpoint. • Disconnected ⇆ - Peripheral is turned off or no longer connected to the endpoint. • Error ⚠ - Endpoint reports an error with the peripheral. • Blank - Endpoint is not reporting that the peripheral is connected.
Paired HDX	Name of the endpoint to which the peripheral is connected or **Not Paired**. The **Not Paired** designation means the peripheral was connected to an endpoint, but it is not connected to one now.
Type	The type of peripheral.
Serial Number	The serial number of the peripheral.
IP Address	The IP address assigned to the peripheral, if applicable.
Area	(Available only when Areas are enabled.) The area with which peripheral is associated. The peripheral inherits its area from the endpoint to which the peripheral is connected. Users can only view area information for the areas to which they belong or have been assigned to manage.
Hardware Version	The hardware version of the peripheral.
Software Version	The software version of the peripheral.

Actions in the Peripheral View

Besides providing access to the peripherals, the **Actions** section of the **Peripheral View** may also include these context-sensitive commands depending on the selected peripheral type and its status.

Action	Use this action to...
Delete Peripheral	(Available only when the peripheral is no longer paired with an endpoint.) Delete the peripheral from the **Peripheral View** list.
Display Applications	(Available only for peripherals on which you can install multiple applications.) Display a list of installed applications and their version.

Add and Monitor Endpoints and Peripherals

The follow topics describe the actions available in **Endpoint > Monitor View**:

- View Endpoint Details on page 93
- Add an Endpoint or Find an Endpoint on the Network on page 97
- Edit an Endpoint on page 101
- Delete an Endpoint on page 102
- Manage Owner of an Endpoint on page 102
- Manage Endpoint on page 102
- View an Endpoint’s Video Feed on page 103
- Clear an Endpoint Help Request on page 103
- Send a Message to an Endpoint on page 104
- Reboot an Endpoint on page 104
- Associate a User with an Endpoint on page 104
- Search for Endpoints in a Range of IP Addresses on page 105
- Monitor Peripherals on page 107

View Endpoint Details

To view detailed information about a managed endpoint

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

   The **Device Details** dialog box displays the following information:

Field	Description
Identification	
Name	The name of the endpoint. • Endpoint names must be unique. • The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. • The system name might be different than the H.323 ID.
Device Type	The type of endpoint. For valid types, see Supported Endpoint Types on page 109.
IP Address	The assigned IP address of the endpoint.
Owner	The person to whom the endpoint is assigned.
Site	The network site for the endpoint. By default, endpoints are added to the **Primary Site**. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Description	A free-form text field (extended ASCII only) in which information about the endpoint can be added.
Serial Number	The serial number (ASCII only) of the endpoint.The endpoint provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.
Bundled Provisioning Profile	The name of the bundled provisioning profile associated with this endpoint. Only available for Polycom HDX systems and Polycom Group systems.
Bundled Profile Description	The description of the bundled provisioning profile associated with this endpoint. Only available for Polycom HDX systems and Polycom Group systems.
HTTP URL	The management URL for the endpoint, if available (ASCII only). This URL allows the RealPresence Resource Manager system to start the endpoint ‘s management system using the **Manage** function. All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the RealPresence Resource Manager system.
HTTP Port	The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.
Area	The area to which the endpoint is assigned. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.

Field	Description
Addresses	
SIP URI	A SIP URI is the address used to call another person via SIP. In effect it's a user's SIP phone number. The SIP URI will be of the following format: `<username>@host(domain or IP):Port`
Aliases	The aliases that allow you to connect to the endpoint. The RealPresence Resource Manager system converts the aliases to the IP address associated with the endpoint. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown. • The endpoint name is the system name, which might be different from the H323 ID. • The value of the E.164 alias is the extension dialed to reach this endpoint. **Note** • The following **Alias Values** are ASCII only: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.
ISDN Video Number	For ISDN endpoints only, the country code + city/area code + phone number for the endpoint. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. Only native ISDN is supported.
LAN Host Name	The host name of the endpoint on the LAN. This can be different from the system name of the endpoint. It is an ASCII only name.
Call Signaling Address	The port on which the gatekeeper associated with the RealPresence Resource Manager system sends call signaling information.
RAS Address	The port on which the gatekeeper associated with RealPresence Resource Manager system sends RAS addressing information.
Capabilities	
Supported Protocols	The communications protocols that the endpoint can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks. • **IP (SIP)** - A standard that defines the protocols used for multimedia communications on SIP networks. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. For endpoints with the type **Unknown**, select **H.323**. The endpoint automatically provides the protocols if it registered successfully or is managed.
Required MCU Service	The MCU service selected for the endpoint to use.

Field	Description
Capabilities Enabled	Capabilities enabled on this endpoint. Options are: • **MCU** - The endpoint can act as a control unit for multipoint conferences • **Gateway** - The endpoint can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed.
Monitoring Level	The monitoring level for the endpoint. Possible values include: • **Standard.** This endpoint is monitored. • **VIP.** This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Available to Schedule	Identifies if the endpoint is available when users are scheduling conferences
Call Info > Sites	
Far Site Name	The H.323 ID of the far site endpoint to which the selected endpoint is connected. When multiple endpoints are connected through the endpoint's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' | ', for example 'ISDN-CO1-7-1 | Vsfx-9-1'.
Far Site Number	The address of the far site endpoint to which the selected endpoint is connected. The address value for the calling endpoint appears to be the dialed address. The address value for the called endpoint appears to be the IP Address.
Encryption	
Cause Code	The cause code showing how the call ended.
Error	
Video FEC Errors	The number of Forward Error Correction (FEC) errors that have been corrected in the current call.
Sync	
Call Type	Type of call, such as, H.323, SIP, ISDN, or POTS.
Call Info > Call Details	
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include: • H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264
Video Format	The video format, both transmission (Tx) and reception (Rx), the endpoint is using.
Video Rate	The video bandwidth negotiated with the far site.

Field	Description
Video Rate Used	The actual video bandwidth used in the call to the far site.
Video Frame Rate	Specifies the frame rate the endpoint is using.
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the endpoint is using. Possible values include: • G.711 • G.722 • G.728
Audio Rate	The audio bandwidth negotiated with the far site
Call Info > Quality of Service (Not reported by all endpoint types)	
Total Packet Loss	Specifies the total packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active call that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Audio Packet Loss	Specifies the audio packet loss for the currently active call.
Video Packet Loss	Specifies the video packet loss for the currently active call.
Audio Jitter	Specifies the audio jitter for the currently active call.
Video Jitter	Specifies the video jitter for the currently active call.
Call Info > Video Feed	
Near Site	The video feed from the endpoint.
Far Site	The video feed from the endpoint to which the endpoint is connected.
System Alerts	
Errors	Endpoint error message, for example, GK Registration error.
Warnings	Endpoint warning message, for example, Low Battery.

Add an Endpoint or Find an Endpoint on the Network

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

This action is not supported for RealPresence Mobile, RealPresence Desktop, RealPresence Group systems and RealPresence Immersive Studio systems.

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

> When a SIP-only endpoint registers with the Polycom DMA system and does not register with the RealPresence Resource Manager system's provisioning service to become dynamically managed, you must manually add it to the RealPresence Resource Manager system in order to manage that endpoint.

To add an endpoint to the system or find an endpoint on the network

1. Go to **Endpoint > Monitor View** and click **Add**.
2. In the **Add New Device** dialog box, select the **Device Type**. For valid types, see Supported Endpoint Types on page 109. For endpoints not specified in the list, select a **Device Type** of **Other**.
3. Enter the **IP Address** of the endpoint.
4. Click **Find Device**.
   - ➢ If the RealPresence Resource Manager system can find the endpoint on the network, the **Add New Device** dialog box is populated with information retrieved from the endpoint. Review any information retrieved from the endpoint.
   - ➢ If the RealPresence Resource Manager system cannot find the endpoint on the network, a **Device Not Found** dialog box appears.

> If you enter an invalid **Admin ID** or **Password** for an endpoint that requires that information, the RealPresence Resource Manager system may still find the endpoint. It depends upon the endpoint type.
>
> - Polycom HDX systems won't allow the RealPresence Resource Manager system to detect the endpoint type and complete the registration. You can manually add the endpoint, but the RealPresence Resource Manager system cannot communicate with it until you've entered a valid **Admin ID** or **Password** for the endpoint. In this case, the RealPresence Resource Manager system records an error message in an error log.
> - The **Find Device** function only works for endpoints with a specified **Device Type**. If you selected a **Device Type** of **Other**, the RealPresence Resource Manager system will report an error.

5. Assign the endpoint a **System Name**.You can edit the system name only if the RealPresence Resource Manager failed to find the endpoint.

   Endpoint names must be unique, must be in ASCII only, and may have an unlimited number of characters. Spaces, dashes, and underscores are valid.
6. If necessary, enter the **Admin ID** and **Password** for the endpoint. Some endpoints may not require this information. Other endpoints may require only a password.

7 Complete the **Identification**, **Addresses,** and **Capabilities** sections of the **Add New Device** dialog box.

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

Note that many fields in this dialog box are ASCII only. Depending on the selected type, some of these fields may not be displayed or may not be editable.

Field	Description
Identification	
Description	A free-form text field (extended ASCII only) in which information about the endpoint can be added.
GAB Display Name	Enter a name for the endpoint as it will appear in the Global Address Book.
Site	The network site for the endpoint.The system determines the site based upon IP address. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Serial Number	The serial number (ASCII only) of the endpoint.The endpoint provides the serial number if it registered successfully or is managed.
Software Version	The version of the software installed on the endpoint (ASCII only). The endpoint provides the version number if it registered successfully or is managed.
HTTP URL	The management URL for the endpoint, if available (ASCII only). This URL allows the RealPresence Resource Manager system to start the endpoint ‘s management system using the **Manage** function. All Polycom endpoints allow management through a browser. For these endpoints, this field is completed when the endpoint registers with the RealPresence Resource Manager system.
HTTP Port	The HTTP port number for the endpoint. The endpoint provides the port number if it registered successfully and is managed.
Assign Area	Assign this endpoint to an area. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage. If the user manages only one area, the endpoint will automatically be assigned to that area.
Addresses	
DNS Name	The name for the endpoint as entered on the domain name server.

Field	Description
SIP URI	The address used to call the endpoint via SIP. `<username>@host(domain or IP):Port`
Aliases	The aliases that allow you to connect to the endpoint. The RealPresence Resource Manager system converts the aliases to the IP address associated with the endpoint. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown. **Notes** • The following **Alias Values** are ASCII only: **H323 ID**, **URL**, **Transport Address**, and **Unknown**. • In other cases, the endpoint name is the system name, which might be different from the H323 ID. • The value of the E.164 alias is the extension dialed to reach this endpoint.
ISDN Video Number	For ISDN endpoints only, the country code + city/area code + local phone number for the endpoint. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The RealPresence Resource Manager system only supports native ISDN.
Capabilities	
Supported Protocols	The communications protocols that the endpoint can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based H.323 networks. • **IP (SIP)** - A standard that defines the protocols used for multimedia communications on SIP networks. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. For endpoints with the type **Unknown**, select **H.323**. The endpoint automatically provides the protocols if it registered successfully or is managed.
Required MCU Service	The MCU service selected for the endpoint to use.
Capabilities Enabled	Capabilities enabled on this endpoint. Options are: • **MCU** - The endpoint can act as a control unit for multipoint conferences • **Gateway** - The endpoint can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed.

Field	Description
Monitoring Level	The monitoring level for the endpoint. Possible values include: • **Standard.** This endpoint is monitored. • **VIP.** This endpoint is monitored closely. The VIP identifier and filters are available to operators to monitor and manage conferences.
Available to Schedule	Identifies if the endpoint is available when users are scheduling conferences

8 Click **Add**.

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

- Add the endpoint to the applicable site.
- Set the **HTTP Port** to `80`
- Add an **Alias** for the endpoint.
- Make the endpoint **Available to Schedule**
- Set the **Monitoring Level** to **Standard**

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

Once you’ve added an endpoint, you can associate it with a user. See Assign Users Roles and Endpoints on page 308.

Edit an Endpoint

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

To edit an endpoint in the RealPresence Resource Manager system

1 Go to **Endpoint > Monitor View**

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

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

4 As required, edit the **Identification**, **Addresses,** and **Capabilities** sections of the **Edit Device** dialog box. For more information, see View Endpoint Details on page 93.

Note that many fields in this dialog box are ASCII only.

5 Click **Update**.

> Editing information for an endpoint on the RealPresence Resource Manager system does not change the information in the endpoint. To make changes in the endpoint information, use **Provisioning** or change it at the endpoint interface.

Delete an Endpoint

To delete an endpoint from the RealPresence Resource Manager system

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoint of interest and click **Delete**.
4. Click **Yes** to confirm the deletion.

   The **Endpoint** list is updated.

Manage Owner of an Endpoint

You can manage the owner of endpoint that uses scheduled management. You cannot manage the owner of an endpoint that is dynamically-managed.

To manage the owner (user associated with the endpoint) of an endpoint

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

   The **Edit User** dialog box appears.
4. Edit any user properties you need.
5. Click **OK**.

Manage Endpoint

You can navigate to the management interface of an endpoint from the RealPresence Resource Manager.

This function is not available for all endpoint types, including RealPresence Desktop, RealPresence Mobile and CMA Desktop.

To manage an endpoint from the RealPresence Resource Manager system

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Click **Manage**.

   A new browser instance opens and navigates to the web interface of the

View an Endpoint’s Video Feed

This procedure is available on the following endpoint types:

- Polycom HDX system
- Polycom RealPresence Group system
- TANDBERG
- VSX-Series

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

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

   The **Device Details** dialog box appears. For information about these fields, see View Endpoint Details on page 93.
4. Click **Call Info** to expand the **Call Info** options and select **Video Feed**.

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

Clear an Endpoint Help Request

This action is only applicable for an HDX system.

To clear an endpoint help request from the RealPresence Resource Manager system

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

   The **Confirm Endpoint Help Clear** dialog box appears.
4. To send a message to the endpoint as well as clear the help request, check **Also send message to endpoint**.
5. Click **Clear**.
6. If you selected the **Also send message to endpoint** check box, enter the text message to send the endpoint in the **Send Message to Endpoint** dialog box and click **Send**.

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

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

Send a Message to an Endpoint

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

This action is not applicable for RealPresence Mobile, RealPresence Desktop or CMA Desktop systems.

To send a message to an endpoint from the RealPresence Resource Manager system

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

   If the endpoint can receive text messages, a **Send Message** option appears in the **Action** menu.
4. Click **Send Message**.
5. In the **Send Message to Endpoint** dialog box, enter a text message and click **Send**.

   The message is sent to the endpoint.

Reboot an Endpoint

In some situations, for example when a remote endpoint is unresponsive, you may need to reboot an endpoint remotely through the RealPresence Resource Manager system.

To reboot an endpoint from the RealPresence Resource Manager system

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Click **Reboot Device**.
5. To confirm the request, click **Reboot**.

Associate a User with an Endpoint

This action is available for endpoints that are not dynamically managed.

To associate an endpoint to a user within the RealPresence Resource Manager system

1. Go to **Endpoint > Monitor View**
2. As needed, use the **Filter** to customize the **Endpoint** list.
3. Select the endpoint of interest.
4. Click **Associate User**.

5 In the **Last Name** field of the **Associate User** dialog box, enter all or part of the user's last name and click **Search**.

   The system displays the list of users who meet your search criteria.

6 Select the user of interest and click **Close**.

Search for Endpoints in a Range of IP Addresses

You can search for endpoints within a range of IP addresses. This search will only include endpoints that are not dynamically-managed.

To search for a set of endpoints within a range of IP addresses

1 Go to **Endpoint > Monitor View** and click **Search Devices**.

2 In the **Search Devices** dialog box, enter the starting IP address and ending IP address for the search range and click **Search**.

   The system begins searching for endpoints. A progress bar displays the status of the search and a results message displays the number of endpoints searched and the number of endpoints found within the IP range.

Download an Endpoint Inventory Report

You can download an inventory report of endpoints if you have the Admin role. This report is in *.CSV format and includes the following information about each endpoint.

Endpoint Attribute	Value
Endpoint Name	The name of the device.
Endpoint Type	The type of device.
Model	The model number of the device
Manage Mode	Describes in the device is dynamically managed: NON_DYNAMIC means it is not dynamically managed. DYNAMIC means the endpoint is dynamically managed.
Owner Name	The user associated with the device.
IP Address	The assigned IP address of the device.
ISDN Video Number	For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The RealPresence Resource Manager system only supports native ISDN.
E.164 Number	The value for the E.164 number associated with this device.
H323 Alias	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.
SIP URI	The SIP URI address for the device.
Software Version	The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.
Serial Number	The serial number (ASCII only) of the device.The device provides the serial number if it registered successfully or is managed.
Sites	The network site for the device. By default, devices are added to the **Primary Site**. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
GK IP	The IP address of the gatekeeper to which the device is registered.
SIP server IP	The IP address of the SIP server to which the device is registered.

To download an endpoint inventory report

1. Navigate to **Endpoint > Monitor**.
2. Click the **Export as CSV** button.
3. Choose to open or save the file.

Monitor Peripherals

The following topics describe the actions available in the **Endpoint > Peripherals View**:

- View Peripherals
- Delete Peripheral
- Display Applications

View Peripherals

If an endpoint has one or more peripherals connected, you can view information about the peripherals.

1 Go to **Endpoint > Monitor View** and select an endpoint that has peripherals connected.

2 Click **View Peripherals**.

3 From the **Peripherals** dialog box, select the peripheral of interest to see the following information.

Field	Description
Paired Endpoint	Name of the endpoint the peripheral is connected to.
Serial Number	The serial number of the peripheral.
IP Address	IP address of the peripheral, if applicable.
Area	The area in which the peripheral is associated. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.
Hardware Version	Version of the peripheral hardware.
Software Version	Version of the peripheral software.
Pairing Status	The status can be one of the following: • Connected • Disconnected
Alert Status	Alert status of the peripheral, if applicable. Not all peripherals report an alert status.

Delete Peripheral

You can delete peripherals from the **Peripherals View** list when the peripheral is no longer connected to an endpoint.

1 Go to **Endpoint > Peripherals View** and select a peripheral that is listed as **Not Paired**.

2 Click **Delete Peripheral**.

3 In the **Confirm Delete** dialog box, click **Yes**.

Display Applications

For peripherals on which you can install multiple applications, you can display a list of installed applications and their version.

1 Go to **Endpoint > Peripherals View** and select a peripheral.

2 Click **Display Applications**.

The **Applications Installed on** dialog box for the selected peripheral appears.

Field	Description
Application Name	Name of the peripheral application.
Version	Version of the peripheral application.

3 Click **Close**.

Supported Endpoint Types

The Polycom® RealPresence® Resource Manager system supports managing and monitoring both Polycom and third-party endpoints.

This section includes the following topics:

- Supported Polycom Endpoints on page 109
- Supported Third-Party Endpoints on page 111
- Considerations for Third-Party Endpoints on page 112

Supported Polycom Endpoints

The following tables describe the Polycom® RealPresence® Resource Manager system support for endpoints based on endpoint type and category of support. See the *Polycom Resource Manager System Release Notes* for more information on tested and supported endpoint versions.

> The Polycom Telepresence M100 systems register as endpoint type of **Other**. As such, the RealPresence Resource Manager can schedule and perform limited monitoring of these systems.

Polycom Endpoint Types	Global Address Book Access	Dynamic Management[c]	Scheduled Management[a]	Scheduling (Dial In only)[d]	Scheduling (Dial in and Dial out)[b]	Monitoring (Standard)[e]	Command and Control[f]	Reports for IP Calls[g]	Reports for ISDN Calls[e]	Can be Managed Behind a Firewall[h]
RealPresence Desktop	N	Y	N	N	Y	Y	N	Y	N	Y
RealPresence Mobile	N	Y	N	N	Y	Y	N	Y	N	Y
CMA Desktop	N	Y	N	N	Y	Y	N	Y	N	Y

Polycom Endpoint Types	**Global Address Book Access**	**Dynamic Management**[c]	**Scheduled Management**[a]	**Scheduling (Dial In only)**[d]	**Scheduling (Dial in and Dial out)**[b]	**Monitoring (Standard)**[e]	**Command and Control**[f]	**Reports for IP Calls**[g]	**Reports for ISDN Calls**[e]	**Can be Managed Behind a Firewall**[h]
RealPresence Group Series (must be dynamically managed)[a]	N	Y	N	N	Y	Y	Y	Y	N	Y
RealPresence Immersive Studio system (must be dynamically-managed)	N	Y	N	N	Y	Y	Y	Y	N	N
HDX Series (dynamic management mode)	N	Y	N	N	Y	Y	Y	Y	Y	Y
HDX Series (scheduled management mode)	Y	N	Y	N	Y	Y	Y	Y	Y	N
VVX Series (dynamic management mode)[b]	N	Y	N	Y	N	Y	N	Y	N	N
VSX Series	Y	N	Y	N	Y	Y	Y	Y	Y	N
QDX Series	Y	N	Y	N	Y	Y	Y	N	Y	N

a. Polycom RealPresence Group systems must be dynamically managed. If the RealPresence Group system is not dynamically managed, it can still connect to the Global Address Book.

b. The Polycom VVX cannot be dynamically provisioned when it is behind a Polycom VBP-ST firewall.

c. Dynamic Management and Scheduled Management are mutually exclusive functionality.

d. Scheduling (Dial In Only) and Scheduling (Dial In and Dial Out) are presented as mutually exclusive functionality. Some endpoints, such as Polycom VVX systems do not have interfaces that can be asked to perform dialing. Some endpoints, such as CMA Desktop clients and VVX systems require external MCU resources for dial-in conferences.

e. Standard RealPresence Resource Manager monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.

f. Command and Control means the RealPresence Resource Manager system can send a command like Send Message and Reboot, and the endpoint can receive and act on the command.

g. Reports for IP Calls are generated as part of standard gatekeeper functionality. Reports for ISDN Calls are additional system functionality. Endpoints that aren't registered with the gatekeeper or ISDN calls send an alert to the device management function to record CDR information. Some legacy endpoints do not send this alert so the CDRs are not written.

h. Supported behind a Polycom VBP, Polycom RealPresence Access Director or Acme SBC device with Access Proxy enabled.

Supported Third-Party Endpoints

Endpoint Type	Global Address Book Access	Dynamic Management[a]	Scheduled Management[a]	Scheduling (Dial In only)[b]	Scheduling (Dial in and Dial out)[b]	Monitoring (Standard)[c]	Command and Control[d]	Reports for IP Calls[e]	Reports for ISDN Calls[e]
Cisco T150 MXP	Y	N	Y	N	Y	Y	Y	Y	N
Cisco 95 MXP	Y	N	Y	N	Y	Y	Y	Y	Y
Cisco C Series	Y	N	Y	N	Y	Y	Y	Y	N
Cisco EX Series	Y	N	Y	N	Y	Y	Y	Y	N
Cisco SX Series	Y	N	Y	N	Y	Y	Y	Y	N
LifeSize Team and Express 200	Y	N	Y	N	Y	Y	Y	Y	Y
Other LifeSize Models	N	N	N	Y	N	N	N	Y	N
Other third-party endpoints: • Sony PCS • Aertha Maia Starr • VCON (Galaxy and Vigo) • VTEL	N	N	N	Y	N	N	N	Y	N

a. Dynamic Management and Scheduled Management are mutually exclusive functionality. Third-party endpoints cannot be dynamically managed.

b. Scheduling (Dial In Only) and Scheduling (Dial In and Dial Out) are presented as mutually exclusive functionality.

c. Standard RealPresence Resource Manager monitoring does not involve using SNMP. It includes endpoint monitoring (online/offline status) and alerts.

d. Command and Control means the RealPresence Resource Manager system can send a Reboot command, and the endpoint can receive and act on the command.

e. Reports for IP Calls are generated as part of standard gatekeeper functionality. Reports for ISDN Calls are additional system functionality. Endpoints that aren't registered with the gatekeeper or ISDN calls send an alert to the device management function to record CDR information. Some legacy endpoints do not send this alert so the CDRs are not written.

Considerations for Third-Party Endpoints

The RealPresence Resource Manager system includes additional command and control for select TANDBERG C Series, Cisco SX series, Cisco EX series, TANDBERG Edge, and LifeSize Team and Express endpoints. The RealPresence Resource Manager system can send a Reboot command to these endpoints, and the endpoints can receive and act on the command. In addition, the RealPresence Resource Manager system can:

- Discover these endpoints by searching for them within a range of IP addresses.
- Complete the initial provisioning of these endpoints.
- Schedule and launch point-to-point conferences on these endpoints.
- Launch the management interface for these endpoints.

In the following sections, some additional considerations for supporting third-party endpoints are discussed, including:

- Reporting and Monitoring for Third-Party Endpoints on page 112
- Considerations for Cisco Endpoints on page 112
- Considerations for LifeSize Endpoints on page 113

Reporting and Monitoring for Third-Party Endpoints

- The RealPresence Resource Manager system includes standard reporting for select Cisco C Series, Cisco SX Series, Cisco EX Series, TANDBERG Edge, and LifeSize Team and Express endpoints.
- The RealPresence Resource Manager system can monitor select Cisco C Series, Cisco SX Series, Cisco EX Series, TANDBERG Edge, and LifeSize Team and Express endpoints, so when properly configured, the RealPresence Resource Manager system can provide online/offline status and alerts, display call status, and provide image support including near and far end images for these endpoints.

Considerations for Cisco Endpoints

Polycom supports managing Cisco endpoints. This section discusses the following topics:

- Enable Cisco Endpoints Global Address Book Access on page 112
- Scheduled Provisioning of Selected TANDBERG and Cisco Endpoints on page 113

Enable Cisco Endpoints Global Address Book Access

With the RealPresence Resource Manager system, users of the Cisco150, 990, 880, 770 MXP, CIsco C Series, Cisco EX Series, Cisco SX Series, and TANDBERG Edge endpoint types can access the Polycom Global Address Book, so they can see the endpoints in the Global Address Book.

The timing of the endpoint’s connection with the Global Address Book can affect the success of its connection. We recommend the following process:

1 At the endpoint, enter the information required for directory set up including the Polycom Global Address Book/RealPresence Resource Manager system IP address and the path.

   For example,
   `http://<RPRM_IP_ADDRESS>/TMS/Public/external/phonebook/PhoneBookService.asmx`

   To do this on Cisco endpoints, go to **System Configuration> Phone Book Server**.

2 Wait for the connections to take effect.

3 At the RealPresence Resource Manager system, go to **Endpoint > Monitor View** and verify the endpoint's Global Address Book connection status is green.

Some notes about the Cisco connection to the Global Address Book:

- Even if the Global Address Book is password protected, Cisco endpoints are not required to provide a password. They have unrestricted access to the Global Address Book.

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

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

Scheduled Provisioning of Selected TANDBERG and Cisco Endpoints

You can set up scheduled provisioning profiles for third-party endpoints. See the appropriate product documentation for more information about these endpoint configuration fields and their acceptable values. See Using Scheduled Provisioning Profiles on page 123 for information on implementing scheduled provisioning of endpoints.

Considerations for LifeSize Endpoints

Consider the following when you must support LifeSize endpoints:

- Enabling Management of a LifeSize Endpoints on page 113
- Provisioning of LifeSize Passwords on page 114
- Scheduled Provisioning of LifeSize Endpoints on page 114

Enabling Management of a LifeSize Endpoints

To facilitate management of a LifeSize endpoints, you must enable the **Default Passwords for LifeSize Endpoint Management** option and enter the SSH and web UI passwords for the LifeSize endpoints.

To enable LifeSize endpoint management

1 On the RealPresence Resource Manager system, go to **Endpoint > Scheduled Management > Endpoint Management Settings**.

2 In the **Default Passwords for LifeSize Endpoint Managemen**t section of the **Endpoint Management Settings** page, enable **Use Default Passwords**.

3 Enter the **Password for SSH User** and confirm the password. Refer to the LifeSize system documentation for information on using SSH to connect to the endpoint, then enter the same SSH password here.

4 Enter the **Password for Web UI User** and confirm the password. Refer to the LifeSize system documentation for information on using a web browser to connect to the endpoint, then enter the same web UI password here.

5 Click **Update**.

Provisioning of LifeSize Passwords

Take note of the following when provisioning passwords to LifeSize endpoints:

- The Auto password must be provisioned to meet the LifeSize and SSH/telnet rules for passwords.
- You cannot provision the Auto password to be blank. If you attempt to provision a blank value, the existing value of the password will not be overwritten. It will remain valid.
- The Web UI or User password can be provisioned to include the numbers 0-9 and/or the symbols * and #. The system will silently truncate these passwords to a maximum of 16 characters.
- You can provision the Web UI or User password to be blank.

Refer to the LifeSize documentation for more information about the requirements for these password.

Scheduled Provisioning of LifeSize Endpoints

The RealPresence Resource Manager system can provision many fields for LifeSize Team and Express endpoints. See the appropriate product documentation for more information about these endpoint configuration fields and their acceptable values. See the Using Scheduled Provisioning Profiles on page 123 for information on implementing scheduled provisioning of endpoints.

Endpoint Device Details

This chapter identifies the fields found in the **Device Detail** section of the Polycom® RealPresence® Resource Manager system interface. It includes these topics:

- Endpoint Device Summary Information on page 115
- Device Status Information on page 117
- Call Information on page 118
- Device Alerts Information on page 119
- Provisioning Details on page 119
- Software Update Details on page 120

Endpoint Device Summary Information

The **Device Summary** information for endpoints in the **Monitor View** section includes the following fields.

Field	Description
Name	The name of the device.
Type	The type of device. For valid device types, see Supported Endpoint Types on page 109.
ID	The system-generated ID for the device.
Owner	(Endpoints only) The user associated with the device.
IP Address	The assigned IP address of the device.
Area	Area with which the device is associated. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.
ISDN Video Number	For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The RealPresence Resource Manager system only supports native ISDN.

Field	Description
Site	The network site for the device. By default, devices are added to the **Primary Site**. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Software Version	The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.
Serial Number	The serial number (ASCII only) of the device.The device provides the serial number if it registered successfully or is managed.
Available to Schedule	Select this option to make the device available when users are scheduling conferences. **Note** The **Available to schedule** field is disabled for RMX 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. • **SIP** - A standard that defines the protocols used for multimedia communications over IP. • 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** check box is selected. If the endpoint supports true ISDN, the **H.323** and **ISDN** check boxes are selected.
Capabilities Enabled	Capabilities to enable on this device. Options are: • **MCU** - The device can act as a control unit for multipoint conferences • **Gateway** - The device can act as a gateway for call management The MCU provides the capability if it registered successfully or is managed.

Field	Description
Alias (type)	The alias to connect to the device. The Resource Manager system converts the aliases to the IP address associated with the device. • **Alias Type**. Possible types include E.164, H.323 ID, URL, Transport Address, E-mail, Party Number, and Unknown. • **Alias Value**. Value for the alias type shown. • 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. • The value of the E.164 alias is the extension dialed to reach this endpoint. • To add another alias, select the type, enter the value (ASCII only), and click **Add Alias**. • To remove an alias, select it and click **Delete Selected Row**. **Note** The following **Alias Values** are ASCII only: **H323 ID**, **URL**, **Transport Address**, and **Unknown**.
SIP URI:	The SIP URI address for the device.

Device Status Information

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

Field	Description
Gatekeeper Registration	The status of the device's registration with the gatekeeper service. Possible values include: • Registered • Unregistered
Directory 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
Exchange Registration	The status of the device's registration with the Microsoft Exchange service.
SIP Registration	The status of the device's registration with the SIP service.
Device Managed	Indicates whether or not the RealPresence Resource Manager system is dynamically managing the device.
Gatekeeper Address	The IP address of the gatekeeper to which the device is registered.

Field	Description
Device Local Time	The local time as set within the device in a default format of `hh:mm:ss AM | PM`. This field is blank for the following device types: **RMX**, **GW/MCU**, **Other**, and **TANDBERG**.
ISDN Line Status Type	The status of the ISDN line. Possible values include: • Operational 🟩 • Non-operations ≠ This field is blank for the following device types: **RMX**, **GW/MCU**, **Other**, and **TANDBERG**.
ISDN Assignment Type	How the ISDN type was assigned to the device. Possible values include: • **Administrator**, when the ISDN type was assigned manually by an administrator • **Endpoint**, when the ISDN type was natively assigned in the endpoint • **Auto-Assigned**, when the ISDN type was automatically assigned by the Resource Manager system based on the site configuration • **From Network**, when the ISDN type was derived from the gateway and extension • **Undefined**, when the Resource Manager system cannot identify the source for the ISDN type assignment This field is blank for the following device types: **RMX**, **GW/MCU**, **Other**, and **TANDBERG**.
Device ISDN Type	The ISDN network interface type installed in the device. Possible values include: • ISDN_QUAD_BRI • ISDN_PRI_T1 • ISDN_BRI • ISDN_UNKNOWN This field is blank for the following device types: **RMX**, **GW/MCU**, **Other**, and **TANDBERG**.

Call Information

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

Field	Description
Call Type	The connection protocol for the call in which the device is participating. Possible values include: H.323, H.320, and SIP.
Video Protocol	The video connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • H.261 H.261 is an ITU standard designed for two-way communication over ISDN lines and supports data rates which are multiples of 64Kbit/s. H.261 supports CIF and QCIF resolutions. • H.263 H.263 is based on H.261 with enhancements that improve video quality over modems. It supports CIF, QCIF, SQCIF, 4CIF and 16CIF resolutions. • H.264

Field	Description
Video Format	The video format, both transmission (Tx) and reception (Rx), the device is using.
Audio Protocol	The audio connection protocol, both transmission (Tx) and reception (Rx), the device is using. Possible values include: • G.711 • G.722 • G.728
Far Site Name	The H.323ID of the far site device to which the selected endpoint is connected. When multiple endpoints are connected through the device's embedded MCU, this field displays a concatenation of each endpoint's H.323ID separated by ' | ', for example 'ISDN-CO1-7-1 | Vsfx-9-1'.
Far Site Number	The address of the far site device to which the selected endpoint is connected. The address value for the calling device appears to be the dialed address. The address value for the called device appears to be the IP Address.
Cause Code	Standard H.323 cause code that reflects normal call termination or the nature of an internal failure, for example, '16' or '211'.
Encryption	Indicates if a call is encrypted or not.
Precedence Level	Applicable only on AS-SIP calls. AS-SIP servers support a “precedence level” that defines a call’s priority in terms of the order in which it is given access to network resources.

Device Alerts Information

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

Field	Description
Errors	Device error message text, for example, GK Registration error
Warnings	Device warning message text, for example, Low Battery

Provisioning Details

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

Field	Description
Last Provisioning Type	The last provisioning type that was used for this endpoint.
Last Provisioning Rule Applied	The name of the last provisioning rule that was applied to this endpoint.
Last Profile Applied	The name of the last provisioning profile that was or was not successfully applied to the device. The **Provisioning Status** will be either **Success** or **Failed**.

Field	Description
Last Bundled Profile Applied	The name of the last bundled profile that was applied to this endpoint.
Provisioning Status	The device's current provisioning status. Possible values include: • **Clear.** No provisioning has been done. • **Pending.** Provisioning is scheduled for this device. • **In Progress.** The device is currently being provisioned. • **Success.** Provisioning has been completed successfully on this device. • **Failed.** Provisioning was not completed on this device. Some endpoint systems expect all configuration fields to be provisioned. If any of the fields are not provisioned, the status will indicate failed. However, the endpoint will often function successfully.
Pending Profile	The name of the provisioning profile that is scheduled to be applied to the device. In this case, the **Provisioning Status** will be either **Pending** or **In Progress**. This field is blank if the device is not scheduled for provisioning.
Scheduled	The date and time, in the default format of `yyyy-mm-dd hh:mm`, when the device is schedule to be provisioned. This field is blank if the device is not scheduled for provisioning.
Last Attempt Date/Time	The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last provisioning message exchanged with the device.
Failure Reason	A text description of the reason the provisioning failed. Causes for failure include: • The provisioning profile does not exist • The provisioning profile does not include provisioning information • The Resource Manager system no longer manages the device • A password for the device is set in the video endpoint system, and you must enter it in the Resource Manager system • The device is busy • A network error occurred • An incomplete transfer of provisioning information occurred • Provisioning has timed out • An internal error occurred on the device, and you must reboot it • An unknown error occurred. Reboot the device.
Log Message	A read-only text box that contains messages related to the device provisioning status

Software Update Details

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

Field	Description
Software Update Status	The device's software update status. Possible values include: • Clear. A software update has not been done. • Pending. A software update has been scheduled and is pending. The device may be offline or in a call. • In Progress. The software update is in progress. • Success. A software update has completed successfully. • Failed. A software update could not be performed.
Scheduled	The date and time, in the default format of `yyyy-mm-dd hh:mm`, when the device software is scheduled to be updated. This field is blank if the device is not scheduled for provisioning.
Last Attempt Date/Time	The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last software update message exchanged with the device.
Failure Reason	A text description of the reason the software update failed. Causes for failure may include: • The software update file location does not exist. • A password for the device is set in the video endpoint system, and you must enter it in Resource Manager. • A network error has occurred. • The update has timed out. • An internal error occurred on the device, and you must reboot it. • A profile has not been configured. • An endpoint is offline. • An incorrect activation key is in the key file. • An unknown error has occurred. Reboot the device
Log Message	A read-only text box that contains the log message text recorded during the execution of the software update. Note that there are no log messages displayed for dynamically-managed endpoints.

Scheduled Endpoint Management

This section provides an introduction to the Polycom® RealPresence® Resource Manager system endpoint management functionality and operations.

Scheduled management allows you to push software updates and provisioning profiles to endpoints at intervals that you define. You can use scheduled management features to manage Polycom as well as third-party endpoints.

Scheduled management uses server-to-client communication over HTTP. This management technique is more appropriate for corporate networks where both the RealPresence Resource Manager and all endpoints are behind the same firewall.

It includes:

Using Scheduled Provisioning Profiles

Scheduling Endpoint Software Updates

Using Scheduled Provisioning Profiles

Scheduled provisioning is enabled at the Polycom® RealPresence® Resource Manager system. To schedule an endpoint for provisioning, the RealPresence Resource Manager system must already have a scheduled provisioning profile created for the endpoint.

This chapter describes RealPresence Resource Manager system endpoint provisioning operations. It includes these topics:

- How Scheduled Provisioning Works on page 123
- Scheduled Provisioning Profiles on page 123
- Scheduled Provisioning Notes on page 124
- Using Scheduled Provisioning on page 125
- Endpoint Fields for Scheduled Provisioning on page 130

How Scheduled Provisioning Works

Users with the Device Administrator or Area Administrator role can schedule provisioning for one endpoint or a group of endpoints; 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 HTTP connection.

Scheduled provisioning is available for these endpoint types:

- VSX Series endpoints
- Selected TANDBERG endpoints—TANDBERG 95 and 150 MXP, and C 20 endpoints
- HDX Series--Polycom HDX systems that are not dynamically managed (are not configured to use a provisioning server)
- Polycom QDX
- LifeSize 200

Scheduled Provisioning Profiles

The RealPresence Resource Manager system does not include a default profile for scheduled provisioning. You must create a profile before you can schedule a endpoint for provisioning. Create a different profile for each endpoint type and group of users.

Some examples of when to use scheduled provisioning profiles follow.

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

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

- To update the password for all endpoints 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 endpoint to update.

For information about how to add a scheduled provisioning profile, see Add a Scheduled Provisioning Profile on page 126.

The sections may differ depending on the endpoint type selected.

Scheduled Provisioning Notes

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

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

You can manually add endpoints to the RealPresence Resource Manager system for monitoring purposes only.

Using Scheduled Provisioning

This section describes the scheduled provisioning tasks a user assigned the Device Administrator can perform. Users with the role of area administrator can perform all tasks EXCEPT adding, editing, and cloning a scheduled provisioning profile.

- Viewing the Scheduled Management List and Details on page 125
- Add a Scheduled Provisioning Profile on page 126
- Edit a Scheduled Provisioning Profile on page 127
- Clone a Scheduled Provisioning Profile on page 127
- Delete a Scheduled Provisioning Profile on page 128
- Schedule an Endpoint for Provisioning on page 128
- Check the Status of a Scheduled Provisioning on page 129
- Clear the Status of Scheduled Provisioning on page 129
- Cancel a Scheduled Provisioning on page 129

Viewing the Scheduled Management List and Details

Navigate to **Endpoint > Scheduled Management > Provisioning** to:

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

To view the list of scheduled provisioning profiles and details about a scheduled provisioning operation

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

Endpoint List in the Scheduled Provisioning View

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

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

Field	Description
Filter	The filter choice for endpoint types that can be scheduled for provisioning. Possible values include: • **HDX Series**—Displays the Polycom HDX systems operating in scheduled management mode. • **LifeSize®** • **QDX Series** • **V and VSX Series**
Status	The status of the endpoint's last provisioning process. Possible values include: • **Success** • **Pending** • **Failed** • **Clear**
Name	The system name of the endpoint.
Type	The type of endpoint. Scheduled provisioning is only available for the endpoints types listed in this table as **Filter** selections.
IP Address	The IP address assigned to the endpoint.
Last	The date and time of the endpoint's last provisioning, unless its status has been cleared.
Pending	When the endpoint is scheduled for provisioning, this field shows the provisioning profile to be used for the scheduled provisioning process.
Scheduled	When the endpoint is scheduled for provisioning, this field shows the date and time for the next scheduled provisioning process.

Add a Scheduled Provisioning Profile

The first step in scheduled provisioning is to create a profile for the endpoint type you want to provision.

To add a scheduled provisioning profile

1. Go to **Endpoint > Scheduled Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, click Add.
3. In the **Add Profile** dialog box, select the **Endpoint Type** for the provisioning profile, enter a name for the profile, and click Add.

4 As needed, select **Provision This Page** and complete the **General Settings, Video Network**, **Monitors**, **Cameras**, **Audio Settings**, **LAN Properties**, and **Global Services** sections of the **Provisioning Fields** dialog box.

   For information about these fields, see Endpoint Fields for Scheduled Provisioning on page 247.

   The sections may differ depending on the endpoint type selected.

5 Click OK.

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

Edit a Scheduled Provisioning Profile

You can edit an existing provisioning profile. You cannot rename an existing profile. If you want to change the name of a provisioning profile, you must use the **Clone** action.

To rename an existing profile, see Clone a Scheduled Provisioning Profile on page 127.

To edit a scheduled provisioning profile

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

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

3 As needed, select **Provision This Page** and complete the **General Settings, Video Network**, **Monitors**, **Cameras**, **Audio Settings**, **LAN Properties**, and **Global Services** sections of the **Provisioning Fields** dialog box.

   For a detailed description of the endpoint fields you can configure when adding a new scheduled provisioning profile, see Endpoint Fields for Scheduled Provisioning on page 247.

   You may find more implementation details about these fields in the endpoint system documentation.

   The sections may differ depending on the endpoint type selected.

4 Click OK.

   The provisioning profile is updated.

Clone a Scheduled Provisioning Profile

If you want to rename an existing provisioning profile or create a new profile based on an existing profile, you can use the **Clone** action.

To clone a scheduled provisioning profile

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

2 In the **Provisioning Profiles** page, select a profile and click Clone.

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.

4 Edit the sections of the **Provisioning Fields** dialog box.

For information about these fields, see Endpoint Fields for Scheduled Provisioning on page 247.

The sections may differ depending on the endpoint type selected. For more information on these fields, see the product documentation for the selected endpoint.

5 Review each page of the scheduled provisioning profile and determine if you want the parameters on the page provisioned. If you do want the parameters on the page provisioned, select **Provision This Page**.

6 Click OK.

The provisioning profile is updated.

Delete a Scheduled Provisioning Profile

You can delete a provisioning profile at any time. Deleted profiles will no longer be sent during scheduled provisioning updates.

To delete a scheduled provisioning profile

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

2 In the **Provisioning Profiles** page, select a profile and click Delete.

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

The profile is deleted from the RealPresence Resource Manager system.

Schedule an Endpoint for Provisioning

You can schedule provisioning profiles to be sent to endpoints at times you specify.

To schedule an endpoint for provisioning

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

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

3 Select the endpoints that you want to schedule provisioning updates.

4 Click **Provision**.

5 In the **Schedule Endpoint Provisioning** dialog box, select the appropriate provisioning profile.

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

7 If you select **Later**, enter a **Date** and **Time** for the provisioning.

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

9 Click **Schedule**.

The **Scheduled Provisioning View** reappears.

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

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

Check the Status of a Scheduled Provisioning

You can check the status of an existing scheduled profile.

Profile statuses include: **Pending**, **Failed**, **Success**, and **Clear**.

To check the status of a scheduled provisioning

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

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

3 Select the endpoint of interest.

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

For a detailed description of the endpoint fields you can configure when adding a new scheduled provisioning profile, see Endpoint Fields for Scheduled Provisioning on page 247. You may find more implementation details about these fields in the endpoint system documentation.

Clear the Status of Scheduled Provisioning

When you clear the status of an endpoint's provisioning status. This allows you to reset the provisioning status so you can better monitor succeeding provisioning updates.

To clear the status of a scheduled provisioning

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

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

3 Select the endpoint of which you want to clear the status.

4 Click **Clear Status**.

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

Cancel a Scheduled Provisioning

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

To cancel a pending scheduled provisioning

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

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

3 Select the endpoints of interest.

4 Click **Cancel Provision**.

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

Endpoint Fields for Scheduled Provisioning

The following table shows the fields you can configure when adding a new scheduled provisioning profile for a Polycom endpoint. You may find more implementation details about these fields in the endpoint system documentation.

For information about third-party endpoint fields, consult the respective documentation.

To view or created scheduled provisioning profiles, select **Endpoint > Scheduled Management > Provisioning Profiles**.

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
General Settings > System Settings > System Settings 1				
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.	Y	Y	Y
Allow Mixed IP and ISDN calls	Specifies whether users can make multipoint calls that include both IP and H.320 sites.	Y	Y	—
Auto Answer Point-to-Point Calls	Specifies whether to set the endpoint system to answer incoming point-to-point calls automatically.	Y	Y	Y
Auto Answer Multipoint Calls	Specifies whether to set the endpoint system to answer incoming multipoint calls automatically.	Y	Y	—
Allow Directory Changes	Specifies whether users can save changes to the directory or contacts/favorites list.	Y	Y	Y
Confirm Directory Additions Upon Call Disconnect	Specifies whether users are prompted to confirm deletions of directory entries.	Y	Y	Y
Confirm Directory Deletions	Specifies whether users are prompted to confirm new directory entries when saving the information for the last site called.	Y	Y	Y
Allow Access to User Setup	Specifies whether the User Settings screen is accessible to users via the System screen. Select this option to allow users to change limited environmental settings.	Y	Y	Y
General Settings > System Settings > System Settings 2				
Far Site Name Display	Specifies how long the far site name to appear on the screen when the call is first connected.	Y	Y	Y
Display Time in Call	Displays time that the current call has been connected	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Keypad Audio Confirmation	Allows the user to hear a voice confirmation of the numbers selected with the remote control.	Y	Y	Y
Call Detail Report	Collects call data.	Y	Y	Y
Recent Calls	Provides navigational tool for call history.	Y	Y	Y
Color Scheme	Enables the customization of the look of the system with five different color schemes.		Y	
Screen Saver Wait Time	The time the system will delay before going into standby mode after nonuse		Y	Y
General Settings > Home Screen Settings > Home Screen Settings 1 Home screen settings cannot be provisioned for Polycom QDX endpoints.				
Dialing Display	Dialing entry field - Includes the dialing entry field on the Home screen. Display Marquee - Allows the addition of text to the dialing entry field of the Home screen.	Y	Y	Y
Enter Marquee Text	Enter the Marquee text that will appear in the “Dialing entry field” when Display Marquee is selected.	Y	Y	Y
Call Quality	Allow users to select the speed/bandwidth of the call.	Y	Y	Y
Display H.323 Extension	Displays the IP dialing extension on the main call screen	Y	Y	Y
Directory	Includes the Directory button on the Home screen.	Y	Y	Y
System	Includes the System button on the Home screen.	Y	Y	Y
Multipoint	Includes the Multipoint navigational item on the Home screen.	Y	Y	
General Settings > Home Screen Settings > Home Screen Settings 2				
System Name	Enable when the system name is to be displayed on the Home Screen.	Y	Y	Y
IP or ISDN Information	• Both – Displays both number types on the system’s Home screen. • IP only – Display the system IP number on the Home screen. • ISDN only – Displays the system ISDN number on the Home screen. • None – The system will not display contact numbers on the Home screen.	Y	Y	
Local Date and Time	Displays the local time on the Home screen.	Y	Y	Y
Enable Availability Control	Displays availability icons on the Home screen.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Sites	Displays icons created for frequently called sites on the Home screen.	Y	Y	Y
Last Number Dialed	Displays the last number dialed on the Home screen.	Y	Y	Y
General Settings > Security				
Remote Access Password	Specifies the password for administrator access when logging in to the system remotely. When the remote access password is set, users must enter it to manage the system from a computer. The remote access password must not contain spaces.	Y	Y	Y
Meeting Password	Specifies the password users must supply to join multipoint calls on this system if the call uses the internal multipoint option, rather than a bridge. The meeting password must not contain spaces. Do not set a meeting password if multipoint calls will include audio-only endpoints. Audio-only endpoints cannot participate in password-protected calls. You cannot provision this setting for Polycom VSX systems.	Y	Y	
Enable FTP Access	Specifies that the endpoint system can be accessed via an FTP session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.		Y	
Enable Web Access	Specifies that the endpoint system can be accessed via it’s web interface. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.	Y	Y	Y
Enable Telnet Access	Specifies that the endpoint system can be accessed via a telnet session. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
AES Encryption	Specifies how to encrypt calls with other sites that support AES encryption. • Off—AES Encryption is disabled. • When Available—AES Encryption is used with any endpoint that supports it, even if the other endpoints in the call don't support it. • Required for Video Calls Only—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are allowed. Video endpoints must support AES Encryption to participate in the call. • Required for All Calls—AES Encryption is used for all video endpoints in the call. Analog phone and voice over ISDN connections are not allowed. All endpoints must support AES Encryption to participate in the call.	Y	Y	Y
Enable SNMP Access	Specifies that the endpoint system can be accessed via an SNMP monitoring system. Note: The system restarts if you change the remote access settings. This setting does not deactivate the associated port, only the application. Use Web Access Port to disable the port.			
General Settings > Date and Time 1				
Date Format	Specifies the preferred format preference for the date and time display and lets you enter your local date and time.	Y	Y	Y
Time Format		Y	Y	Y
Month		Y	Y	Y
Day		Y	Y	Y
Year		Y	Y	Y
Hour		Y	Y	Y
Minute		Y	Y	Y
AM/PM		Y	Y	Y
Auto Adjust for Daylight Saving Time	Specifies the daylight savings time setting. When this setting is enabled, the system clock automatically changes for daylight saving time.	Y	Y	Y
Time Difference from GMT	Specifies the time difference between GMT (Greenwich Mean Time) and the endpoint system's location.	Y	Y	Y
Time Server	Specifies connection to a time server for automatic system time settings.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Primary Time Server Address	Specifies the address of the time server to use when Time Server is set to Manual.	Y	Y	Y
Video Network > IP Network > Call Preferences				
Enable IP H.323	Allows the system to make IP calls	Y	Y	Y
Enable H.239	Specifies standards-based People+Content data collaboration. Enable this option if you know that H.239 is supported by the far sites you will call. If callers experience issues when sharing content with other Polycom systems, disable this setting.	Y	Y	Y
Enable Transcoding	Specifies whether the system allows each far-site system to connect at the best possible call rate and audio/video algorithm. If transcoding is disabled, the Polycom HDX system down-speeds all connections to the same call rate.	Y	Y	
ISDN Gateway	Allows users to place IP-to-ISDN calls through a gateway.	Y	Y	Y
IP Gateway	Allows users to place ISDN-to-IP or IP-to-IP calls through a gateway.	Y	—	
Video Network > IP Network > Gatekeeper				
Use Gatekeeper	Specifies whether to use a gatekeeper. Gateways and gatekeepers are required for calls between IP and ISDN. • **Off** — Calls do not use a gatekeeper. • **Auto** — System attempts to automatically find an available gatekeeper. • **Specify** — Calls use the specified gatekeeper. Enter the gatekeeper's IP address or name (for example, gatekeeper.companyname.usa.com, or 10.11.12.13).	Y	Y	Y
Gatekeeper IP Address	If you chose to use an automatically selected gatekeeper, this area displays the gatekeeper's IP address. If you chose to specify a gatekeeper, enter the IP address.	Y	Y	Y
Use Gatekeeper for Multipoint Calls	Specify whether multipoint calls use the system's internal multipoint capability or the Conference on Demand feature.	Y	Y	
Video Network > IP Network > Gateway Number				
Country Code	Specifies the country code for the system's location	Y	Y	
Area Code	Specifies the area or city code for the system's location	Y	Y	
Gateway Number	Specifies the gateway's number	Y	Y	

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Gateway Number Type	Specifies the number type users enter to call this system: • Direct Inward Dial — Users enter an internal extension to call this system directly. **Note** If you choose this setting, you must also register the number with the gatekeeper as an E.164 alias. • Number + Extension — Users enter the gateway number and the system's extension to call this system.	Y	Y	
Number of digits in DID Number	Specifies the number of digits in the DID number. The national or regional dialing plan for your location determines the standard number of digits. For instance, the US standard is 7 digits.	Y	Y	
Number of digits in Extension	Specifies the number of digits in the extension used when Direct Inward Dial is selected. Your organization's dial plan determines this number.	Y	Y	
Video Network > IP Network > Quality of Service Settings				
Type of Service Field	Specifies the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedenc**e — Represents the priority of IP packets sent to the system. The value can be between 0 and 7. • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.	Y	Y	Y
Video Type of Service Value	Specifies the IP Precedence or Diffserv value for video packets. This value does not apply to the CMA Desktop system. It's value is set by the client's operating system.	Y	Y	Y
Audio Type of Service Value	Specifies the IP Precedence or Diffserv value for audio packets.	Y	Y	Y
FECC Type of Service Value	Specifies the IP Precedence or Diffserv value for Far End Camera Control packets.	Y	Y	Y
Enable Dynamic Bandwidth	Specifies whether to let the system automatically find the optimum line speed for a call	Y	Y	
Enable PVEC	Allows the system to use PVEC (Polycom Video ErrorConcealment) if packet loss occurs.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Video Network > IP Network > Firewall Settings				
Use Fixed Ports	Specifies whether to define the TCP and UDP ports. • If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. • If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. **Note** You must open the corresponding ports in the firewall. You must also open the firewall's TCP port 1720 to allow H.323 traffic.	Y	Y	Y
Start TCP Port	Allows you to 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. **Note** You must also open the firewall's TCP port 1720 to allow H.323 traffic.	Y	Y	Y
Start UDP Port	Allows you to 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.	Y	Y	Y
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**.	Y	Y	Y
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.	Y	Y	Y
NAT is H.323 Compatible	Specifies that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Address Displayed in Global Directory	Specifies whether or not to include the endpoint system’s information in the global directory	Y	Y	Y
Video Network > ISDN BRI Protocol				
Enable ISDN H.320	Allows this system to make H.320 (ISDN) calls.	Y	Y	
Number of ISDN Channels to Dial in Parallel	Specifies how many channels to dial at one time. You can specify up to eight channels. If you experience network problems, decrease the number. Set this value to 1 for serial dialing. Serial dialing is not recommended unless you have trouble connecting calls using parallel dialing.	Y	Y	
ISDN Switch Protocols	Specifies the protocol used by your network’s switch.	Y	Y	
Outside Line Dialing Prefix	Specifies the ISDN dialing prefix used to call outside the network.	Y	Y	
Video Network > Preferred Speeds				
Preferred Speed for Placing Calls (Kbps)	Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when: • The **Call Quality** selection is either unavailable or set to **Auto** on the **Place a Call** screen • The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.	Y	Y	Y
IP Calls		Y	Y	Y
ISDN Video Call (H.320)		Y	Y	
International ISDN calls		Y	Y	
Maximum Speed for Receiving Calls (Kbps)	Allows you to restrict the bandwidth used when receiving IP or ISDN calls. If the far site attempts to call the system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field.	Y	Y	Y
IP Calls		Y	Y	Y
ISDN Video Call (H.320)		Y	Y	
Monitors > Monitors 1				
Number of Monitors				Y
Monitor 1 Options				
Monitor 1	Specifies the monitor’s aspect ratio. • 4:3 — Select if you are using a regular TV monitor.			Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Video Format	Specifies the monitor’s format: • DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. • VGA — Select if the monitor is connected to the DVI connector using a VGA cable. • Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors. • S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. • Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.	Y	Y	
Display Icons in Call	Specifies whether to display all on-screen graphics, including icons and help text, during calls.	Y	Y	Y
Snapshot Timeout	Lets you choose whether to have slides and snapshots time out after a period of four minutes.	—	Y	
Dual Monitor Emulation	Specifies whether the system can show multiple views on a single display.	Y	Y	
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates. • Select **Black** to display black video. This is the recommended setting to prevent burn-in for TV monitors. • Select **No Signal** to have the display react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors.	Y		Y
VGA Resolution		—	Y	
Monitor 2 Options	**Applies to:**	Y	—	Y
Monitor 2	Specifies the second monitor’s aspect ratio: • Off — Select if you do not have a second monitor. • 4:3 — Select if you are using a regular TV monitor as the second monitor.	Y	—	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Video Format	Specifies the monitor’s format: • DVI — Select if the monitor is connected to the DVI connector using a DVI or HDMI cable. • VGA — Select if the monitor is connected to the DVI connector using a VGA cable. • Component YPbPr — Select if the monitor is connected to the DVI connector using component cables. Polycom HDX 8000 series and Polycom HDX 7000 series systems do not support 720p Component format for 50 Hz monitors. • S-Video (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using an S-Video cable. • Composite (Polycom HDX 9000 series only) — Select if the monitor is connected to the BNC connectors using a composite video cable.	Y	—	Y
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the monitor when the system goes to sleep and the screen saver activates. • Select **Black** to display black video. This is the recommended setting to prevent burn-in for TV monitors. • Select **No Signal** to have the display react as if it is not connected when the system goes to sleep. This is the recommended setting for VGA monitors and projectors.	Y	—	Y
People Display Mode				Y
Content Display Mode				Y
Color System				Y
Monitor 3 Options				
Monitor 3	Specifies the aspect ratio for recording. • Off — Select if you do not have a VCR or DVD player connected to record video conferences. • 4:3 — Select to record for playback on a standard monitor. • 16:9—Select to record for playback on a wide-screen monitor, if your recording device has this capability. See the endpoint product documentation for more information about these selections.	Y	—	

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Video Format	Specifies the VCR or DVD player’s format: • S-Video — Select if the VCR or DVD player is connected to a Polycom HDX system using an S-Video cable. • Composite — Select if the VCR or DVD player is connected to a Polycom HDX system using a composite video cable and S-Video to RCA adapter.	Y	—	
Output Upon Screen Saver Activation	Specifies whether black video or no signal is sent to the VCR or DVD player when the system goes to sleep and the screen saver activates. • Select **Black** to send black video. • Select **No Signal** to have the VCR or DVD player react as if it is not connected when the system goes to sleep.	Y	—	
VCR/DVD Record Source	Specifies the video source to be recorded to videotape or DVD. • If **Far** is enabled, the recorded video will switch to the current far site speaker. • If both **Near** and **Far** are enabled, the recorded video will switch between near and far sites depending on the current speaker. • If **Content** is enabled, any content sent during the call is recorded.	Y	—	
Near		Y	—	
Far		Y	—	
Content		Y	—	
Screen Saver Wait Time	The time the system will delay before going into standby mode after nonuse	Y		
Cameras > Cameras 1				
Far Control of Near Camera	Specifies whether the far site can pan, tilt, or zoom the near-site camera. When this option is selected, a user at the far site can control the framing and angle of the camera for the best view of the near site.	Y	Y	Y
Backlight Compensation	Specifies whether the camera should automatically adjust for a bright background. Backlight compensation is best used in situations where the subject appears darker than the background.	Y	Y	Y
Primary Camera	Specifies which camera is the main camera.	Y	Y	Y
Camera Direction	Specifies the direction the camera moves when using the arrow buttons on the remote control.	Y	Y	Y
Cameras > Camera Settings				
Camera 1 Name	Specifies a name for camera 1.	Y	Y	Y
Camera 1 Icon	Specifies an icon for camera 1.	Y	Y	Y
Camera 2 Name	Specifies a name for camera 2.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Camera 2 Icon	Specifies an icon for camera 2.	Y	Y	Y
Camera 3 Name	Specifies a name for camera 3.	Y	Y	Y
Camera 3 Icon	Specifies an icon for camera 3.	Y	Y	Y
Cameras > Video Quality				
Camera 1	Specifies Motion or Sharpness for the video input. The default is Sharpness. • **Motion** — This setting is for showing people or other video with motion. • **Sharpness** — The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped. Sharpness is available in point-to-point H.263 and H.264 calls only. It is recommended for HD calls between 1 Mbps and 2 Mbps.	Y	Y	Y
Camera 2		Y	Y	Y
Camera 3		Y	Y	Y
Audio Settings > Audio Settings 1				
Sound Effects Volume	Sets the volume level of the ring tone and user alert tones.	Y	Y	Y
Incoming Video Call	Specifies the ring tone used for incoming calls.	Y	Y	Y
User Alert Tones	Specifies the tone used for user alerts.	Y	Y	Y
Mute Auto Answer Calls	Specifies whether to mute incoming calls. Incoming calls are muted by default until you press the mute on the microphone or on the remote control.	Y	Y	Y
Line Input	Specifies the type of equipment that is connected to audio input 1.	Y	Y	
Input Type Level	Sets the volume level for audio input 1.	Y	Y	
Line Input Level	Sets the volume level for audio input 2.	Y	Y	
Line Outputs	Specifies how the audio output behaves. The default selection, **Monitor - Far Site Audio**, supplies audio to the Monitor 1 audio outputs only when the system is receiving audio from the far site. If you have connected a VCR to record the conference, select **Monitor - Far and Near Audio** to supply audio from both the far site and the system’s microphones.	Y	Y	
Line Output Level	Sets the volume level for audio output	Y	Y	
Audio Settings > Audio Settings 2				
Master Audio Volume	Sets the volume level for audio from the far site.	Y	Y	Y

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Midrange Speakers	Specifies whether to use the system’s built-in midrange speaker. You may prefer to turn off the midrange speaker if you connect the audio output to Monitor 1 or if you connect an external speaker system.	—	Y	
Bass	Sets the volume level for the low frequencies without changing the master audio volume.	Y	Y	
Treble	Sets the volume level for the high frequencies without changing the master audio volume.	Y	Y	
LAN Properties > LAN Properties 1				
Connect to My LAN	Enables connection to the local area network	Y	Y	
IP Address	Specifies how the system obtains an IP address. • **Obtain IP Address Automatically** — Select if the system gets an IP address from the DHCP server on the LAN. • **Enter IP Address Manually** — Select if the IP address will not be assigned automatically.	Y	Y	Y
Use the Following IP Address	If you selected **Enter IP Address Manually**, enter the IP address here.	Y	Y	Y
LAN Properties > LAN Properties 2				
DNS Servers	Displays the DNS servers currently assigned to the system. If the system does not automatically obtain a DNS server address, enter up to four DNS servers here. Changing this setting causes the system to restart.	Y	Y	Y
Default Gateway	Displays the gateway currently assigned to the system. If the system does not automatically obtain a gateway IP address, enter one here. Changing this setting causes the system to restart.	Y	Y	Y
Subnet Mask	Displays the subnet mask currently assigned to the system. If the system does not automatically obtain a subnet mask, enter one here. Changing this setting causes the system to restart.	Y	Y	Y
WINS Server	Displays the server running the Windows Internet Name Service	—	Y	
WINS Resolution	Enables connection to the WINS Server for URL resolution	—	Y	

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
LAN Speed	Specify the LAN speed to use. Note that the setting you choose must be supported by the switch. Choose Auto to have the network switch negotiate the speed automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets Duplex Mode to Auto. If you choose 10 Mbps, 100 Mbps, or 1000 Mbps you must set Duplex Mode to Half or Full. Changing this setting causes the system to restart. **Note** Mismatches with the network switch settings may lead to unexpected behaviors.	Y	Y	Y
Duplex Mode	Specify the duplex mode to use. Note that the Duplex mode you choose must be supported by the switch. Choose Auto to have the network switch negotiate the Duplex mode automatically. In this case, the switch must also be set to Auto. Choosing Auto automatically sets LAN Speed to Auto. Changing this setting causes the system to restart.	Y	Y	Y
Global Services > Directory Servers				
Global Directory (GDS)	Specifies the IP address or DNS address of the Global Directory Server.	Y	Y	Y
Password	Lets you enter the global directory password, if there is one.	Y	Y	Y
Display Name in Global Directory	Specifies whether to display the system’s name in the global directories of other registered systems. Global Address	Y	Y	Y
Display Global Addresses	Displays other registered systems in the global directory.	Y	Y	Y
Register	Registers this system with the Global Directory Server.	Y	Y	Y
Save Global Directory to System	Copies the global directory to this local system. When this setting is disabled, the system can display no more than 1,000 global directory entries. When this setting is enabled, the system can display up to 4,000 global directory entries.	Y	Y	Y
LAN/H.323 > Global Directory (GDS) > Preferences				
Show Addresses in Address Book		—	—	

Field	For the endpoint systems being provisioned...	HDX Series	VSX Series	QDX Series
Preferred Speed for Placing Calls (Kbps)	Determines the speeds that will be used for IP, ISDN, or International ISDN calls from this endpoint system when: • The **Call Quality** selection is either unavailable or set to **Auto** on the **Place a Call** screen • The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed.	—	—	
ISDN Video Call (H.320)		—	—	
International ISDN calls		—	—	
IP Calls		—	—	
LAN/H.323 > Global Directory (GDS) > Preferred Alias				
Preferred Alias	Possible values include: • Gateway Number • ISDN Number • Called Party Line Identifier • Extension	—	—	
Global Services > Account Validation				
Require Account Number to Dial	Specify whether to require an account number for placing calls and whether that number should be validated by the system.	Y	Y	
Validate Account Number	Specify whether to require an account number for placing calls and whether that number should be validated by the system.	Y	Y	
Global Services > My Info				
Contact Person	Specifies the name of the person responsible for this system	Y	Y	Y
Contact Number	Specifies the phone number of the person responsible for this system	Y	Y	Y
Contact Email	Specifies the email address of the person responsible for this system	Y	Y	Y
Contact Fax	Specifies the Fax number of the person responsible for this system	Y	Y	Y
Tech Support	Specifies the contact information for Technical Support for this system	Y	Y	Y
City	Specifies the location of the person responsible for this system	Y	Y	Y
State/Province		Y	Y	Y
Country		Y	Y	Y

Scheduling Endpoint Software Updates

The Polycom® RealPresence® Resource Manager system's software update feature, which requires a software update profile for the endpoint 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 endpoint individually.

The RealPresence Resource Manager system supports two exclusive software update processes: dynamic and scheduled. Dynamic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for dynamic software update should not be scheduled for software updates through the system.

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

This chapter describes how to use Polycom RealPresence Resource Manager system to schedule software updates for endpoints. It includes these sections:

- Software Update Considerations for Multi-Tenancy on page 145
- Creating Scheduled Software Updates for Endpoints on page 146
- Using Scheduled Software Updates on page 149

Software Update Considerations for Multi-Tenancy

Within a multi-tenancy environment, area administrators are not allowed to create software updates or set up maintenance windows for dynamic software updates. However, they are allowed to schedule software updates that have already been uploaded by a user with the administrator role.

Software update images are also not area-aware, which means that users with area administrator roles see all software updates on the system, not just those for their area. As a best practice, the system administrator should either name the software update appropriately or add information to the description field of the update so that area administrators know which updates to use for their area.

Creating Scheduled Software Updates for Endpoints

To implement scheduled software updates, you must first create respective software updates for your endpoints.

Only users with the administrator role can create software updates.

You must create scheduled software updates using the **Endpoint > Scheduled Management > Upload Software Update** menu.

To create a software update, perform this series of tasks.

1. List the Serial Numbers for the Endpoints to be Updated on page 146.
2. Download the Required Software Package on page 147.
3. Request Update Activation Keys on page 148.
4. Upload the Software Update on page 149.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

1. Go to **Endpoint > Scheduled Management > Upload Software Updates.**
2. Select the endpoint type for which to get serial numbers.
   a. If getting serial numbers for a scheduled update, select the appropriate **Endpoint Type** and **Endpoint Model** combination for the endpoint to update. You can select more than one Endpoint.
   b. If getting serial numbers for a dynamic software update, click the appropriate tab for the endpoint.
3. Click **Get Serial Numbers**.

   The **Endpoint Serial Number List** appears listing the endpoints of the selected type and model that are eligible for software updates.

Field	Description
Name	The name assigned to the endpoint system
IP Address	The IP address assigned to the endpoint.
Version	The current software version installed on the endpoint.
Site	The site to which the endpoint belongs. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.

4. As needed, use the **Filter** to customize the endpoint list.
5. Select the specific endpoints to be updated.

6 Click **Get Serial Numbers**.

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

7 Create a `.txt` file containing the serial number(s).

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

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

b Save the `.txt` file.

c Return to the endpoint serial number list and click **Close**.

The **Software Updates** list reappears.

8 Repeat steps Select the endpoint type for which to get serial numbers. through Create a .txt file containing the serial number(s). for the each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same `.txt` file.

9 Click **Close**.

The **Software Updates** list reappears.

Download the Required Software Package

To download the software package required to update the endpoints

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

2 For Polycom endpoints:

a Open a web browser and go to `http://support.polycom.com.`

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

c Select the software package and save it to the directory created in step On your local system, create a directory to which to save the software package (if one does not already exist)..

d Repeat steps a through c for each endpoint type to be updated. Note that the software package may contain the software for different models of the same endpoint type.

3 For third-party endpoints, follow the company’s recommended procedure for downloading a software package. Save it to the directory created in step On your local system, create a directory to which to save the software package (if one does not already exist)..

Request Update Activation Keys

To request upgrade activation keys

1 For Polycom products

a Go to `http://support.polycom.com`.

b Log in or Register for An Account.

c Select **Product Activation**.

d In the **Software Upgrade Key Code** section, click **Retrieve Software KeyCode**.

e When upgrading a single endpoint:

- Enter the serial number of the endpoint to be updated into the **Serial Number** field of the **Single Upgrade Key Code** section.
- Enter the version number to which you are upgrading and click **Retrieve**.
- The key code is returned on the screen.
- Record the key code and create a `.txt` file with the Serial Number - Key Code combination to be updated.
- Close the **Product Activation** screens.

f When updating multiple endpoints from a prepared `.txt` file (step Copy and paste the serial numbers from the endpoint serial number list to a .txt file that you can submit to the Polycom Product Activation site. Put one serial number per line as shown in the following example.):

- In the **Multiple Upgrade KeyCode** section, click **Add Attachment**.
- Browse to the location of the `.txt` file you created in step Copy and paste the serial numbers from the endpoint serial number list to a .txt file that you can submit to the Polycom Product Activation site. Put one serial number per line as shown in the following example. and click **Upload**.
- A file containing the Serial Number - Key Code combinations will be E-mailed to the specified E-mail account.
- When you receive the `.txt` file, save it to your local system.
- Close the **Product Activation** screens.

2 For third-party endpoints, follow the company's recommended procedure for requesting an upgrade activation key.

Upload the Software Update

Note

The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To upload the software package and create an software update profile

1 Go to **Endpoints > Scheduled Management > Upload Software Updates.**

2 Select an endpoint type to update.

3 Click **Upload Software Update**.

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

5 If an activation key code is required to activate the software update, 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 148).

> 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://support.polycom.com`.

6 In the **Software Update File** field, browse to the software update file you downloaded.

7 Enter a meaningful description that will help other users to understand the purpose of the software update.

8 Click **OK**.

A software update profile for the endpoint type and model type is created.

Using Scheduled Software Updates

The scheduled software update feature is enabled at the RealPresence Resource Manager system. An administrator with **System Setup** permissions can schedule software updates for one endpoint or a group of endpoints to occur immediately or for a date and time in the future.

Some notes about scheduled software updates:

- Until the RealPresence Resource Manager system successfully updates an endpoint scheduled for updating, the update remains in the **Pending** or **In Progress** state and the RealPresence Resource Manager system attempts to update the endpoint until it succeeds or until the update is canceled.
- If an endpoint scheduled for update is **In a Call**, the RealPresence Resource Manager system waits until the call ends before updating the endpoint. The system checks the endpoint at 15 minute intervals.
- If an endpoint scheduled for update is **Offline**, the RealPresence Resource Manager system attempts to connect to the endpoint every hour until the endpoint is **Online**.
- A software update may reboot the endpoint.

This section includes these topics:

- Supported Endpoints for Scheduled Software Updates on page 150
- Schedule the Software Update for Endpoints on page 150
- Scheduled Software Update View on page 151
- View Scheduled Software Update Information on page 153
- View List of Software Update Packages on page 153

Supported Endpoints for Scheduled Software Updates

Scheduled software updates are available for these endpoint types.

- HDX Series--when operating in scheduled management mode (not using a provisioning server)
- LifeSize
- Cisco T150
- Cisco C-Series
- Cisco SX-Series
- Cisco EX-Series
- Cisco MXP series

Schedule the Software Update for Endpoints

Only users with the administrator role can schedule software updates. Users with the area administrator role cannot schedule software updates.

To schedule one or more endpoints for software update

1. Go to **Endpoint > Scheduled Management > Schedule Software Updates**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoints of interest and click **Software Update**.
4. In the **Schedule Software Update** dialog box, specify when the update should occur.
   a. In the **Schedule** field, select **Now** or **Later**.
   b. If you select **Later**, enter a **Date** and **Time** for the update.
   c. Select either **Use Server Date/Time** or **Use Endpoint Date/Time** as these may differ.
5. Select from these options.

Fields	Description
Remove address book entries	Select this check box to have all local address book entries removed after the update.
Remove system files	Select this check box to have all endpoint settings removed after the update. You must then reconfigure the endpoint.
Allow endpoint to be a DHCP server	

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

6. Click **Schedule**.

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

Scheduled Software Update View

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

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

Endpoint List in the Scheduled Software Update View

By default the **Endpoint** list in the **Scheduled Software Update View** displays all endpoints eligible for scheduled software update.

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

Field	Description
Filter	Filter choices for this view include: • **Type**—Filters the list by endpoint type. • **Name**—Searches the list by the endpoint’s system name. • **IP Address**—Searches the list by endpoint’s IP address. • **ISDN Video Number**—Searches the list by endpoint’s ISDN video number. • **Alias**—Searches the list by endpoint’s alias. • **Site**—Searches the list by site location. • **Area**—Filters the endpoint list by area. This filter is only available when areas are enabled and when the user manages more than one area.
Status	The status of the endpoint’s last scheduled software update. Possible values include: • **Success** • **Failed** • **Clear**
Name	The system name of the endpoint.
Model	The type of endpoint. Scheduled software update is only available for these endpoint types: • **HDX Series**—Displays the Polycom HDX systems operating in scheduled management mode. • **LifeSize®** • **QDX Series** • **TANDBERG T150** • **TANDBERG C-Series** • **TANDBERG MXP**
IP Address	The IP address assigned to the endpoint.

Field	Description
Current Version	The version of software installed during the last successful software update procedure.
Scheduled	When the endpoint is scheduled for software update, this field shows the date and time for the scheduled software update process.

Scheduled Software Update View Actions

Besides providing access to the endpoint views, the **Action** section for the **Scheduled Software Update View** will also include these actions:

Action	Use this action to...
Software Update	Schedule software update for the selected endpoints.
Cancel Update	Cancel a scheduled or in progress software update operation.
Clear Status	Change the status column for an endpoint to the **Clear** state.

For information about these endpoint actions, see Scheduling Endpoint Software Updates on page 145.

View Scheduled Software Update Information

To view information about software updates that are scheduled or for endpoints that are eligible for scheduled software updates

1. Go to **Endpoint > Scheduled Management > Schedule Software Update**.
2. As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Dial String**, and **Site**.
3. Select the endpoint of interest.
4. In the **Endpoint Summary** pane, expand the **Software Update Details** tab. For more information, see Software Update Details on page 120.

View List of Software Update Packages

To view the list of scheduled software update packages

» Go to **Endpoint> Scheduled Management > Upload Software Updates**.

The **Upload Software Updates** page appears listing all of the endpoint types and models for which the RealPresence Resource Manager system can perform a scheduled software update. It includes this information. If a software update package has been uploaded to the system, the Description and Uploaded fields are populated for the endpoint.

Cancel Software Updates

You can cancel scheduled software updates for an endpoint. You must do that at the endpoint.

To cancel scheduled software updates

1. Go to **Endpoint > Scheduled Management > Schedule Software Updates**.
2. As needed, use the **Filter** to customize the endpoint list.
3. Select the endpoint or endpoints of interest and click **Cancel Update**.

   A confirmation dialog box appears. The dialog box may indicate that one or more of the selected endpoints had a software update in progress.
4. Click **Ok** to cancel in progress and future software updates for the selected endpoints and clear their status.

   You can cancel software update operations that are in progress, but you may wish to check the endpoint afterward to verify it was left in a operational state.

Dynamic Endpoint Management

This section provides an introduction to the Polycom® RealPresence® Resource Manager system dynamic endpoint management functionality and operations. It includes:

Understanding Dynamic Endpoint Management

When you dynamically manage an endpoint, you can remotely control the configuration settings and software version of an endpoint, according to policies you define.

Administrators now have the flexibility of a rule-based system to apply dynamic provisioning profiles. An administrator can create multiple rules and associate a profile with more than one rule at a time. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied.

Dynamic management allows a Polycom endpoint to poll the Polycom ® RealPresence® Resource Manager automatically to get provisioning updates (configuration settings) and software updates on a regular basis.

Dynamic management is client-to-server over HTTPS which makes it more secure and firewall-friendly.

Dynamic management is available:

- Only for Polycom endpoints.
- When Polycom endpoints are able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager to your DNS server.

In dynamic management mode, when a endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package or provisioning profile. If a either is found, the package URL is sent in XML format over a secure HTTPS connection.

Endpoints do not poll the system if they are in a call. They restart polling after the call ends.

This chapter provides an overview on dynamic management.

Supported Polycom Endpoints and Peripherals

You can only dynamically-manage some Polycom endpoints. The following Polycom endpoints and peripherals can be dynamically-managed:

- Polycom VVX system

- Polycom HDX system
- HDX Touch Control
- CMA Desktop (must be dynamically-managed)
- RealPresence Group systems (must be dynamically-managed)
- RealPresence Immersive Studio systems (must be dynamically-managed)
- RealPresence Group Touch Control
- RealPresence Mobile (must be dynamically-managed)
- RealPresence Desktop (must be dynamically-managed)

> Do not use scheduled provisioning profiles for endpoints that are dynamically managed. You should use either scheduled or dynamic provisioning for an endpoint, never both.
>
> Most Polycom endpoints can be dynamically managed (use the RealPresence Resource Manager as their provisioning server).

Overview of Dynamic Management Set Up

Setting up dynamic management of Polycom endpoints is a multi-step process. You'll need to have your DNS server configured, the endpoint needs to be configured to use the RealPresence Resource Manager as its provisioning server, and you'll have to set up provisioning profiles and software updates.

The following topics provide an overview of each step:

- Configure your DNS Server on page 157
- Configure Endpoints to use a Provisioning Service on page 158
- Define Endpoint Naming Schemes on page 158
- Create Provisioning Profiles on page 158
- Create Provisioning Rules on page 158
- Create Access Control Lists on page 159
- Create Software Updates on page 159

Configure your DNS Server

Configure the DNS server, if you wish it to resolve queries for the RealPresence Resource Manager by the RealPresence Resource Manager's host name or IP address.

To dynamically manage endpoints (which includes dynamic provisioning, dynamic software update, and presence), they must be able to automatically discover the RealPresence Resource Manager. This means you must add the DNS service record (SRV record) for the RealPresence Resource Manager.

Configure Endpoints to use a Provisioning Service

At the physical endpoint, configure the endpoint to use the RealPresence Resource Manager as its provisioning service.

You do this via the endpoint’s web interface or soft endpoint’s utility. You can do this on initial setup or at any time when you need to switch to dynamic management.

Some Polycom endpoints must be dynamically-managed, such as RealPresence Desktop, RealPresence Mobile, RealPresence Group systems, and RealPresence Immersive Studio systems.

Define Endpoint Naming Schemes

The RealPresence Resource Manager allows administrators to configure their E.164 alias, system naming schemes and SIP URIs for endpoints that are dynamically managed.

If you choose to provision H.323 settings through a network provisioning profile, you can also define the E.164 number and system naming scheme used for endpoints. You can also auto-generate SIP URIs for dynamically-managed endpoints.

See Dynamically Managing Endpoint Naming Schemes on page 208.

Create Provisioning Profiles

Dynamic provisioning allows endpoints to poll the RealPresence Resource Manager automatically to get provisioning updates (configuration settings) on a dynamic basis. The provisioning profiles the endpoint receives are based provisioning rules you define.

When you dynamically manage endpoints (have the endpoint use the RealPresence Resource Manager as its provisioning server), you can automatically configure them by using provisioning profiles.

You need to modify and create three types of endpoint provisioning profiles:

- **Network Provisioning** profiles define Network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on, see Network Provisioning Profiles on page 185.
- **Admin Config** Provisioning profiles define endpoint administrative settings such as maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on, see Admin Config Provisioning Profiles on page 194.
- **Bundled Provisioning** profiles allow you to control system settings that affect user experience, see Using Bundled Provisioning Profiles on page 217.

Create Provisioning Rules

You can create rules that include conditions that need to be met before the RealPresence Resource Manage system sends a provisioning profile to an endpoint. You can also prioritize these rules so that certain provisioning profiles get applied first.

For more information about provisioning rules, see Creating Dynamic Provisioning Rules on page 199.

Create Access Control Lists

Access Control Lists provide an additional level of endpoint provisioning security when you dynamically manage endpoints. These lists allow you to group endpoints into “white lists” that can be dynamically provisioned. This is particular useful when controlling Polycom’s soft endpoints such as CMA Desktop and RealPresence Mobile which use the provisioning credentials to authenticate with your video network. With Polycom RealPresence Mobile clients, you can also control access according to model (for example, RealPresence Mobile for the iPad).

See Using Access Control Lists on page 231.

Create Software Updates

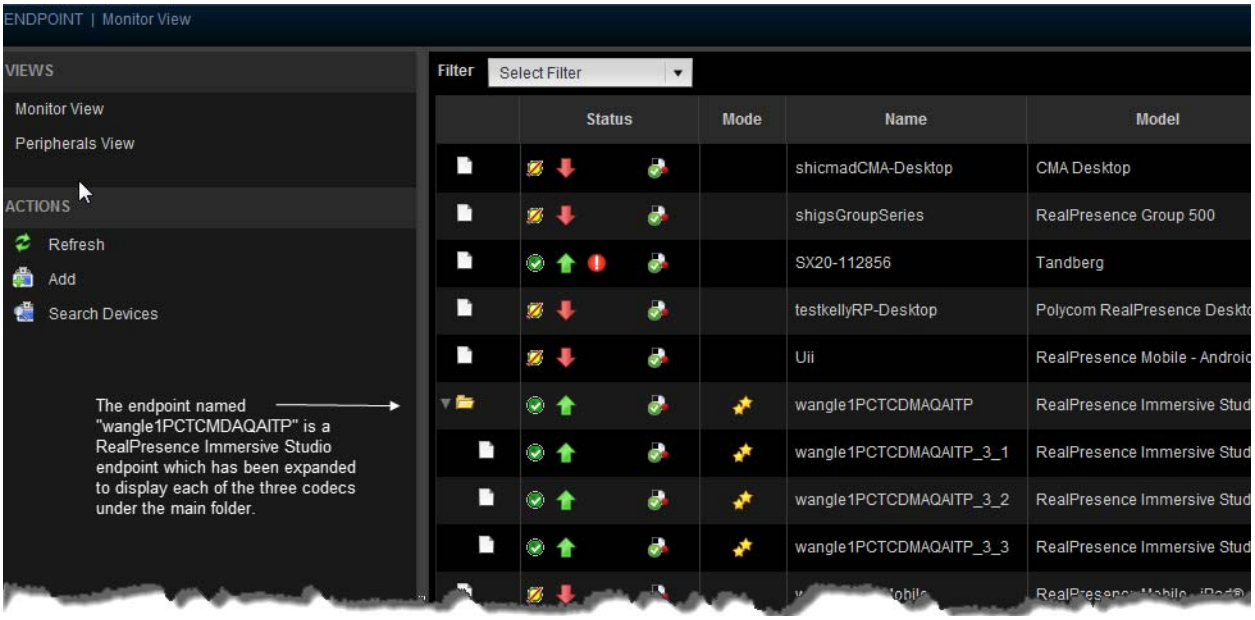
You need to create software updates to automatically send to endpoints. See Dynamically Updating Endpoint and Peripheral Software on page 161 for more information.

Dynamically Managing RealPresence Immersive Studio Systems

A RealPresence Immersive Studio system contains multiple endpoints (codecs). When the RealPresence Resource Manager system dynamically manages (required) these devices, they display as a group of three codecs that following a specific numbered naming convention that helps specify the total number of codecs included in the system. This is in addition to any system name you have configured. For example, the three RealPresence Group systems in an RealPresence Immersive Studio system named **wangle1PCTCDMAQAITP** could display in the RealPresence Resource Manager system screens and reports with the following names:

wangle1PCTCDMAQAITP_3_1
wangle1PCTCDMAQAITP_3_2
wangle1PCTCDMAQAITP_3_3

In the **Endpoint > Monitor** screen, dynamically managed RealPresence Immersive Studio systems display as expandable icons as shown below:



The endpoint named "wangle1PCTCMDAQAITP" is a RealPresence Immersive Studio endpoint which has been expanded to display each of the three codecs under the main folder.

	Status	Mode	Name	Model
	↓		shicmadCMA-Desktop	CMA Desktop
	↓		shigsGroupSeries	RealPresence Group 500
	✓ ↑ !		SX20-112856	Tandberg
	↓		testkellyRP-Desktop	Polycom RealPresence Deskto
	↓		Uii	RealPresence Mobile - Androic
▼	✓ ↑	★	wangle1PCTCDMAQAITP	RealPresence Immersive Stud
	✓ ↑	★	wangle1PCTCDMAQAITP_3_1	RealPresence Immersive Stud
	✓ ↑	★	wangle1PCTCDMAQAITP_3_2	RealPresence Immersive Stud
	✓ ↑	★	wangle1PCTCDMAQAITP_3_3	RealPresence Immersive Stud

The RealPresence Resource Manager system also provisions settings as applying to a single system. You can only provision the primary codec (the device designated as 1); the RealPresence Resource Manager system automatically propagates any changes to the other devices in the ITP system.

Stopping Dynamic Management of an Endpoint

If you want to stop dynamically managing a RealPresence Group Series or RealPresence Immersive Studio endpoint, you must first disable the provisioning service settings on the endpoint.

To stop dynamically managing an endpoint

1. From the endpoint’s web interface, navigate to the Provisioning Service settings and un check the **Enable Provisioning** check box.
2. From the RealPresence Resource Manager system, navigate to **Endpoint > Monitor view**, highlight the endpoint and click **Delete** from the ACTIONS menu.

Dynamically Updating Endpoint and Peripheral Software

The Polycom® RealPresence® Resource Manager system's software update feature, which requires a software update profile for the endpoint 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 endpoint individually.

The RealPresence Resource Manager system supports two exclusive software update processes: dynamic and scheduled. Dynamic and scheduled software update are exclusive endpoint management scenarios. Endpoints enabled for dynamic software update should not be scheduled for software updates through the system.

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

This chapter describes how to use Polycom RealPresence Resource Manager system to dynamically update the software on Polycom endpoints when a new software package is available using a policy you define. It includes these sections:

- Software Update Considerations for Multi-Tenancy on page 161
- Create Dynamic Software Updates for Endpoints on page 162
- Using Dynamic Software Updates on page 166
- Set up a Trial an Dynamic Software Update on page 172
- Dynamic Software Updates for Peripherals on page 175

Software Update Considerations for Multi-Tenancy

Within a multi-tenancy environment, area administrators are not allowed to create software updates or set up maintenance windows for dynamic software updates. However, they are allowed to schedule software updates that have already been uploaded by a user with the administrator role.

Software update images are also not area-aware, which means that users with area administrator roles see all software updates on the system, not just those for their area. As a best practice, the system administrator should either name the software update appropriately or add information to the description field of the update so that area administrators know which updates to use for their area.

Software Update Considerations for RealPresence Desktop

When you upgrade RealPresence Desktop clients, Polycom recommends that you temporarily configure the RealPresence Resource Manager system to reclaim soft endpoint licenses in a very short time (five minutes). As soon as the client's license is reclaimed and re-distributed, the RealPresence Resource Manager system can accurately track the upgraded endpoints

When you upgrade the RealPresence Desktop and RealPresence Mobile clients, you may see erroneous endpoint reports in the RealPresence Resource Manager system that show duplicate RealPresence Desktop endpoints. In addition, these erroneous duplicate endpoints will each consume a RealPresence Desktop license.

After upgrading your RealPresence Desktop and RealPresence Mobile clients, you can reconfigure the license reclamation to the value you need. The default is 30 days.

Create Dynamic Software Updates for Endpoints

To implement a dynamic software update, you must first create respective software updates for your endpoints.

Only users with the administrator role can create dynamic software updates.

> The dynamic software update feature is only available for these endpoint types:
>
> - Polycom HDX system endpoints deployed in dynamic management mode
> - Polycom RealPresence Group systems deployed in dynamic management mode
> - Polycom RealPresence Immersive Studio systems
> - Polycom CMA Desktop systems (Windows and Mac)
> - RealPresence Desktop systems (Windows and Mac)
> - Polycom VVX systems
> - Polycom Touch Controls for both HDX and Group systems when dynamically-managed
>
> Polycom provides default dynamic software update profiles for both CMA Desktop and RealPresence Desktop clients. Default software update profiles are not available for other endpoint systems.

To create a dynamic software update, perform this series of tasks.

1. List the Serial Numbers for the Endpoints to be Updated on page 163.
2. Download the Required Software Package on page 164.
3. Request Update Activation Keys on page 164.
4. Upload the Software Update on page 165. For more information on software update profiles, see View Software Update Details for an Endpoint on page 169.

List the Serial Numbers for the Endpoints to be Updated

To list the serial numbers for the endpoints to be updated

1. Go to **Endpoint > Dynamic Management > Upload Software Updates**.
2. Select the endpoint type for which to get serial numbers.

   You can do this for HDX and Group Series endpoints only.
3. Click **Get Serial Numbers**.

   The **Endpoint Serial Number List** appears listing the endpoints of the selected type and model that are eligible for software updates.

Field	Description
Name	The name assigned to the endpoint system
IP Address	The IP address assigned to the endpoint.
Version	The current software version installed on the endpoint.
Site	The site to which the endpoint belongs. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated. Users can only view area information for the areas to which they belong or have been assigned to manage.

4. As needed, use the **Filter** to customize the endpoint list.
5. Select the specific endpoints to be updated.
6. Click **Get Serial Numbers**.

   The serial number(s) appear in the text box on the page.
7. Create a `.txt` file containing the serial number(s).

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

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

   b. Save the `.txt` file.

   c Return to the endpoint serial number list and click **Close**.

   The **Software Updates** list reappears.

8 Repeat steps Select the endpoint type for which to get serial numbers. through Create a .txt file containing the serial number(s). for the each endpoint or set of endpoints to be updated. You may include all of the serial numbers for all of the different endpoint types in the same `.txt` file.

9 Click **Close**.

   The **Software Updates** list reappears.

Download the Required Software Package

To download the software package required to update the endpoints

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

2 For Polycom endpoints:

   a Open a web browser and go to `http://support.polycom.com.`

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

   c Select the software package and save it to the directory created in step On your local system, create a directory to which to save the software package (if one does not already exist)..

   d Repeat steps a through c for each endpoint type to be updated. Note that the software package may contain the software for different models of the same endpoint type.

3 For third-party endpoints, follow the company's recommended procedure for downloading a software package. Save it to the directory created in step On your local system, create a directory to which to save the software package (if one does not already exist)..

Request Update Activation Keys

To request upgrade activation keys

1 Go to `http://support.polycom.com`.

2 Log in or Register for An Account.

3 Select **Product Activation**.

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

5 When upgrading a single endpoint:

   a Enter the serial number of the endpoint 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**.

   c The key code is returned on the screen.

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

 e Close the **Product Activation** screens.

6 When updating multiple endpoints from a prepared `.txt` file (step a):

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

 b Browse to the location of the `.txt` file you created and click **Upload**.

 c A file containing the Serial Number - Key Code combinations will be E-mailed to the specified E-mail account.

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

7 Close the **Product Activation** screens.

Upload the Software Update

> **Note**
>
> The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To upload the software package and create an software update

1 Go to **Endpoint > Dynamic Management > Upload Software Updates**.

2 Select an endpoint type to update.

3 Click **Upload Software Update**.

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

5 If an activation key code is required to activate the software update, 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 164).

> 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.
>
> Do not modify or rename the file that Polycom sends.
>
> Customers can review their key history at `http://support.polycom.com`.

6 In the **Software Update File** field, browse to the software update file you downloaded.

7 Enter a meaningful description that will help other users to understand the purpose of the software update.

8 Click **OK**.

A software update profile for the endpoint type and model type is created.

Using Dynamic Software Updates

Dynamic software updates, which controls the endpoint's software version level, is tied to the endpoint type and the policy you define. Currently, the dynamic software update feature is only available for these endpoint types.

- Polycom HDX system endpoints that are dynamically-managed
- Polycom RealPresence Group system endpoints that are dynamically-managed
- Polycom RealPresence Immersive Studio systems that are dynamically-managed
- Polycom CMA Desktop systems (both Windows and Mac)
- RealPresence Desktop systems (both Windows and Mac)
- Polycom VVX systems
- Polycom Touch Controls that are dynamically-managed
- Polycom RealPresence Group Series Touch Controls

In dynamic management mode, when a endpoint starts up and at designated intervals thereafter, it automatically polls the RealPresence Resource Manager system for a newer software update package. If a software update is necessary, the package is sent in XML format over a secure HTTPS connection.

Endpoints do not poll for software update packages if they are in a call. They restart polling after the call ends.

This section describes how to use the RealPresence Resource Manager system to dynamically update the software on Polycom endpoints when a new software package is available. It includes these sections:

- Set an Dynamic Software Update Policy on page 166
- View Dynamic Software Update Status on page 168
- View Software Update Details for an Endpoint on page 169
- View Dynamic Software Update Packages on page 170
- Set Maintenance Window for Dynamic Software Updates on page 171

Set an Dynamic Software Update Policy

After creating a dynamic software update, you can use the **Version to use** and **Allow this version or newer** selections to manage the roll out of a software update package. These selections also allow you to manage the release of multiple software packages for the same endpoint type.

Here's how it works: All endpoints 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 dynamic software update.
2. Then to activate the roll out, you change the **Version to use** selection from the current value to the new version number and **Update** the page.

The next time a dynamically managed endpoint polls the RealPresence Resource Manager 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 software update package. Use this method to force users to use a specific software version.

> Until the **Version to use** selection is enabled, the dynamic software update is not activated.

If you also enable the **Allow this version or newer** selection, anytime you upload a newer version of software into a dynamic software update that update 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 RealPresence Resource Manager system, the system will compare the current software version number with the packaged software version numbers. The 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 endpoints 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 RealPresence Resource Manager system will send the specifically identified software package to the endpoint even if it is an older version.

> To roll back a Polycom CMA Desktop or RealPresence 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.

To set a dynamic software update policy for an endpoint type

1. Go to **Endpoint > Dynamic Management > Upload Software Update**.
2. Select the tab for the endpoint type of interest.
3. Choose one of these policies:
   - To specify an area to which to apply the update, use the **Select Area** drop-down to select the area to apply the policy.

     This feature is only available when areas are enabled and you manage more than one area.
   - To specify a minimum version of dynamic software update package, make that version the **Version to use** and select **Allow this version or newer**.
   - To require a specific version of dynamic software update package, make that version the **Version to use** and clear **Allow this version or newer**.
   - To turn dynamic software update off for an endpoint type, change the **Version to use** value to **(none)**.
4. Click **Update**.

View Dynamic Software Update Status

You can view the list of endpoints that have registered to the system for dynamic software updates.

To view the list of endpoints registered to the system for dynamic updates

1. Navigate to **Endpoint** > **Dynamic Management > Software Update Status** menu to view the list of endpoints that have registered to the system for dynamic software updates.
2. Choose a **Filter** to use for the list. Filter choices for this view include:
   - **Type**—Filters the list by endpoint type.
   - **Name**—Searches the list by the endpoint’s system name.
   - **IP Address**—Searches the endpoint list by IP address.
   - **ISDN Video Number**—Searches the endpoint list by ISDN video number.
   - **Dial String**— Searches the endpoint list by dial string (SIP, H.323, or ISDN).
   - **Site**—Searches the endpoint list by site location.
   - **Area**—Filters the endpoint list by area. This filter is only available when areas are enabled and when the user manages more than one area.
3. Use the **Items per page** drop-down to customize the number of endpoints included per page.

   The endpoint list includes the following information:

Field	Description
Status	The status of the endpoint’s last software update. Possible values include: • **Success** • **Failed** • **Clear** • Timed Out • Skipped (only applied to CMA Desktop and RealPresence Desktop clients)
Name	The system name of the endpoint.
Type	The type of endpoint. Dynamic software update is only available for these endpoint types: • HDX systems (when dynamically managed) • RealPresence Group systems (when dynamically managed) • RealPresence Immersive Studio systems (when dynamically managed) • CMA Desktop • RealPresence Desktop • Polycom VVX
IP Address	The IP address assigned to the endpoint.

Field	Description
Current Version	The current software version that the endpoint is using.
Area	(Available only when Areas are enabled.) The area with which the endpoint is associated. You can only view area information for the areas you have been assigned to manage. If you do not manage more than one area, this column is not displayed.

View Software Update Details for an Endpoint

Users with the Device Administrator, Administrator or the Area Administrator role can view details about dynamic software updates made to endpoints.

To view detailed information for endpoints that are eligible for dynamic software updates

1. Go to **Endpoint > Dynamic Management > Software Update Status**.

   The **Software Update Status** page appears.

2. As needed, use the **Filter** to customize the endpoint list. Filter choices include **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Dial String**, **Site** and **Area**.
3. Select the endpoint of interest.
4. In the right pane, expand the **Software Update Details** window.

   The endpoint list in the **Dynamic Software Details** pane has the following information.

Field	Description
Software Update Status	The device’s software update status. Possible values include: • Clear. A software update has not been done. • Pending. A software update has been scheduled and is pending. The device may be offline or in a call. • In Progress. The software update is in progress. • Success. A software update has completed successfully. • Failed. A software update could not be performed.
Last Attempt Date/Time	The date and time, in the default format of `yyyy-mm-dd hh:mm:ss`, of the last software update message exchanged with the device. **Note** Polycom CMA Desktop systems and RealPresence Desktop clients are updated at the start of each session.

Field	Description
Scheduled	For dynamic updates, this value is N/A. For scheduled updates, the date and time, in the default format of `yyyy-mm-dd hh:mm`, when the device software is schedule to be updated. This field is blank if the device is not scheduled for provisioning.
Failure Reason	A text description of the reason the software update failed. Causes for failure may include: • The software update file location does not exist. • A password for the device is set in the video endpoint system, and you must enter it in RealPresence Resource Manager system. • A network error has occurred. • The update has timed out. • An internal error occurred on the device, and you must reboot it. • A profile has not been configured. • An endpoint is offline. • An incorrect activation key is in the key file. • An unknown error has occurred. Reboot the device
Log Message	A read-only text box that contains the log message text recorded during the execution of the software update. Note that there are no log messages displayed for dynamically-managed endpoints.

For more information, see Software Update Details on page 120.

View Dynamic Software Update Packages

To view the list of dynamic software update packages

1 Go to **Endpoint > Dynamic Management > Upload Software Update.**

The **Dynamic Software Policies** page appears and the uploaded software update packages are displayed. The **Dynamic Software Updates** page includes this information.

Field	Description
Select Area	Allows you to specify an area to which to apply the update. This option is only available when areas are enabled and for areas that the user is allowed to manage.
Endpoint Type	The type of endpoint system. You can use dynamic software updates for the following Polycom endpoints and peripherals: • HDX Series • RealPresence Group Series • RealPresence Immersive Studio systems • CMA Desktop (PC and Mac OS) • RealPresence Desktop (PC and Mac OS) • VVX • Polycom HDX Touch Control • RealPresence Group Series Touch Control
Version to use	Displays the default dynamic software update profile to be used for the endpoint type and model.
Allow this version or newer	When checked, indicates that when a newer dynamic software update package for the endpoint type and model is added, that package should be used as the default package.
Version	The version of the software package associated with the dynamic software update package.
Description	The meaningful name given to the dynamic software update package when it was created.
Uploaded	The date and time when the dynamic software update package was created.
Trial Group	The trial group assigned to the software update package, if applicable.

2 To view the dynamic software update packages for other endpoints and peripherals, click the appropriate tab: **HDX, Group Series**, **CMA Desktop** (PC or Mac OS), **VVX** or **HDX Touch Control**, **Group Series Touch Control**, and **RealPresence Desktop** (PC or Mac OS)**.**

Set Maintenance Window for Dynamic Software Updates

You can restrict dynamic software updates of dynamically-managed endpoint systems to a scheduled maintenance window.

Typically, dynamic software updates occur as specified by the Software Update Polling Interval that is provisioned with the network provisioning profile for the endpoint.

Enabling the maintenance window feature in the RealPresence Resource Manager system overrides the **Software Update Polling Interval**. The RealPresence Resource Manager system provisions the maintenance window to the endpoints, and the endpoints hold their dynamic software update requests until the maintenance window starts.

Some notes about this feature:

- It applies to dynamically-managed HDX and RealPresence Group systems only.
- To avoid dynamically updating the software on all HDX or RealPresence Group systems at the start of the maintenance window, the systems randomize their dynamic software update requests.

To restrict dynamic software updates to a scheduled maintenance window

1 Go to **Endpoint Management > Dynamic Management > Upload Software Update.**

2 Click the appropriate tab: **HDX** or **Group Series.**

3 Click **Maintenance Window** in the **ACTIONS** pane.

4 In the **Maintenance Window** dialog box, click **Enable Maintenance Window** and set a maintenance window **Start Time** and either an **End Time** or **Duration**.

   Set the maintenance window start time to the endpoint's system local time, not the RealPresence Resource Manager system local time. For example, if you set the maintenance window start time to 3am, the maintenance window for each HDX system will start at 3am local time. Therefore, the maintenance window for HDX systems in Buffalo, NY will start at 3am EST; the maintenance window for HDX systems in Denver, CO will start at 3am MST; and the maintenance window for HDX systems in San Francisco, CA will start at 3am PST.

5 Click **Save**.

Set up a Trial an Dynamic Software Update

Setting up a trial of a software update requires the user to create a software update. Only users with the administrator role can do this.

To trial a software update package:

1 Get the things you need to create the package. You must have the administrator role to complete the tasks in this step:

   a List the Serial Numbers for the Endpoints to be Updated on page 163.

   b Download the Required Software Package on page 164.

   c Request Update Activation Keys on page 164.

2 Set up testing. Complete these tasks:

   a Create a Local Trial Group on page 173.

   b Upload the Software Package and Create a Trial Software Update Package on page 173. For more information on software update packages, see View Software Update Details for an Endpoint on page 169.

3 Once your testing of the trial software package is complete, do one of these tasks:

   ➢ Promote the Trial Software Update Package to Production on page 174

   ➢ Delete the Trial Software Update Package on page 174.

Create a Local Trial Group

To trial a software update with a specific group of local and/or enterprise users, create a local group that includes these users, as described in Add a Local Group on page 305. The people in this group will receive the trial software update package when their endpoint goes through its normal, automated software update process.

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

Upload the Software Package and Create a Trial Software Update Package

> **Note**
>
> The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To upload the software package and create a trial dynamic software update package

1. Go to **Endpoint > Dynamic Management > Upload Software Update.**
2. Select the tab for the endpoint type of interest.
3. Click **Upload Software Update**.
4. In the **Upload Software Update** dialog box, verify the endpoint type and model.
5. If an activation key code is required to activate the software update, click the **Update Requires Key** check box and in the **Software Update Key File** field browse to the `.txt` key file received in Request Update Activation Keys on page 164.

> 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.
>
> Do NOT rename the file that Polycom sends you.
>
> Customers can review their key history at `http://support.polycom.com`.

6. In the **Software Update File** field, browse to the software update file you want to use.
7. Enter a meaningful description that will help other users to understand the purpose of the software update.
8. To trial the software with the group created previously, select **Trial Software** and from the **Select Trial Group** menu, select the trial group created in Create a Local Trial Group on page 173.

9 Click **OK**.

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

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

Promote the Trial Software Update Package to Production

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

To promote a trial software update package to production

1 Go to **Endpoint> Dynamic Management > Upload Software Updates**.

2 Select the tab for product to update.

3 If areas are enabled, use the **Select Area** drop-down list to choose the area to which to promote the update.

This drop-down list is only available if you manage more than one area.

4 Select the software update package of interest and click **Promote to Production**.

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

The package becomes a production dynamic software update package.

Delete the Trial Software Update Package

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

To delete a trial software update package

1 Go to **Endpoint > Dynamic Management > Upload Software Updates**

2 Select the tab for product to update.

3 Select the software update package of interest and click **Delete Software Update**.

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

The package is removed from the **Dynamic Software Updates** list.

5 To return your trial group to the last production version of software, clear the **Allow this version or newer** option and click **Update**.

6 When all endpoints are back to the last production version of software, reset your dynamic software update policy. See Set an Dynamic Software Update Policy on page 166.

Dynamic Software Updates for Peripherals

You can update the platform (operating system) and applications (if applicable) for peripherals connected to endpoints. Peripheral software updates can be in any of the following states:

- **Production** - The software update is configured for one or more groups that are using the software in production.
- **Trial** - The software update is configured for one or more groups that are trialing the software.
- **Both** - The software update is configured for one or more groups that are trialing the software and for one or groups are using the software in production.

For peripherals that permit software updates from the RealPresence Resource Manager system, you can download the updates from `http://support.polycom.com` and make them available from the RealPresence Resource Manager system web server. You also configure which updates are for trial or production use. The following topics describe software updates for peripherals:

- View Software Updates for Polycom Touch Controls
- Upload Peripheral Software Updates to the RealPresence Resource Manager System
- Configure Peripheral Updates for Production
- Configure Peripheral Updates for Trial

View Software Updates for Polycom Touch Controls

To view software updates for peripherals

1. Go to **Endpoint > Dynamic Management > Upload Software Updates**.
2. Select the **HDX Touch Control** or **Group Series Touch Control** tab.

   The tab includes this information.

Field	Description
Select Area	Allows you to specify an area to which to apply the update.
Production URL	URL where the peripheral can access software updates configured for production use. The URL consists of the IP dress of the RealPresence Resource Manager system plus /repo.
Trial URL	URL where the peripheral can access software updates configured for trial use. The URL consists of the IP dress of the RealPresence Resource Manager system plus /repotrial.
Package Name	Displays the name of the software update package. Updates listed as **platform** are updates to the peripheral’s operating system. Other updates are for specific applications.
Description	The meaningful name given to the software update package when it was created

Field	Description
Version	The version of the software package
Status	The status of the software update. Possible values are: • **None** - The software update has not been configured for production or trial. • **Production** - The software update is configured for production. It is available only from the **Production URL**. • **Trial** - The software update is configured for trial. It is available only from the **Trial URL**. • **Both** - The software update is configured for both production and trial. It is available from both the **Production URL** and the **Trial URL**.
Uploaded	The date and time when the software update package was uploaded

Upload Peripheral Software Updates to the RealPresence Resource Manager System

After you download the software updates from `http://support.polycom.com` and save them on your hard drive, you can upload them to the RealPresence Resource Manager system web server.

> **Note**
> The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To upload software updates to the RealPresence Resource Manager system

1. Go to **Endpoint > Dynamic Management > Upload Software Updates**.
2. Select the tab for the peripheral.
3. Click **Upload Software Update**.
4. In the **Select File to Upload** dialog box, navigate to and select the software update that you saved to your hard drive.
5. Click **Open**.

   The update is added to the list on the peripheral tab.

> If this is the first update for the platform or an application, the update is automatically configured for production.

Configure Peripheral Updates for Production

To configure software updates for production

1. Go to **Endpoint > Dynamic Management > Upload Software Updates**.

2 Select the tab for the peripheral.

3 Click **Configure Production**.

The **Configure Production** dialog box includes the following information.

Field	Description
Configure Platform	
Platform Description	The meaningful name given to the platform software update package when it was created
Status	The current status of the platform software update. Possible values are: • **None** - The software update has not been configured as production or trial. • **Production** - The software update is configured as production. It is available only from the **Production URL**. • **Trial** - The software update is configured as trial. It is available only from the **Trial URL**. • **Both** - The software update is configured as both production and trial. It is available from both the **Production URL** and the **Trial URL**.
Configure Application	
Application Description	The meaningful name given to the application software update package when it was created
Platform Compatible	Column title shows the version of the currently selected platform. Use the drop-down list to select available application versions that match the platform version.
Status	The current status of the application software update. Possible values are: • **None** - The software update has not been configured as production or trial. • **Production** - The software update is configured as production. It is available only from the **Production URL**. • **Trial** - The software update is configured as trial. It is available only from the **Trial URL**. • **Both** - The software update is configured as both production and trial. It is available from both the **Production URL** and the **Trial URL**.

4 From the **Configure Platform** section, select the platform version to configure for production.

You can select only one platform version for production.

5 Click **Configure Application**.

6 For each application, select the version to configure for production from the **Platform Compatible** drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for production.

7 Click **OK**.

From the peripheral itself, the configured software updates are now available using the **Production URL**.

Configure Peripheral Updates for Trial

To configure software updates for trial

1 Go to **Endpoint > Dynamic Management > Upload Software Updates**.

2 Select the tab for the peripheral.

3 Click **Configure Trial**.

The **Configure Trial** dialog box includes the following information.

Field	Description
Configure Platform	
Platform Description	The meaningful name given to the platform software update package when it was created
Status	The current status of the platform software update. Possible values are: • **None** - The software update has not been configured as production or trial. • **Production** - The software update is configured as production. It is available only from the **Production URL**. • **Trial** - The software update is configured as trial. It is available only from the **Trial URL**. • **Both** - The software update is configured as both production and trial. It is available from both the **Production URL** and the **Trial URL**.
Configure Application	
Application Description	The meaningful name given to the application software update package when it was created

Field	Description
Platform Compatible	Column title shows the version of the currently selected platform. Use the drop-down list to select available application versions that match the platform version.
Status	The current status of the application software update. Possible values are: • **None** - The software update has not been configured as production or trial. • **Production** - The software update is configured as production. It is available only from the **Production URL**. • **Trial** - The software update is configured as trial. It is available only from the **Trial URL**. • **Both** - The software update is configured as both production and trial. It is available from both the **Production URL** and the **Trial URL**.

4 From the **Configure Platform** section, select the platform version to configure for trial.

You can select only one platform version for trial.

5 Click **Configure Application**.

6 For each application, select the version to configure for trial from the **Platform Compatible** drop-down list.

The version selected must be compatible with the platform version listed in the column heading. If the application is not selected (no check mark), the application will not be configured for trial.

7 Click **OK**.

From the peripheral itself, the configured software updates are now available using the **Trial URL**.

Using Provisioning Profiles

The Polycom® RealPresence® Resource Manager system allows you to use provisioning profiles and provisioning rules as a way to dynamically manage endpoint settings.

Note

If your deployment includes a RealPresence Access Director that you want to dynamically manage, you must create an RPAD Server Provisioning Profile, see, Dynamically Managing a RealPresence Access Director System on page 241.

This chapter describes how to set up endpoint provisioning profiles within the RealPresence Resource Manager system. It includes these topics:

Setting Up Dynamic Provisioning Profiles

When you dynamically manage endpoints (have the endpoint use the RealPresence Resource Manager as its provisioning server), you can automatically configure them by using provisioning profiles.

Dynamic provisioning profiles are applied through a rule-based paradigm. This change makes provisioning profiles more flexible and allows the administrator more control over when they are applied.

Dynamic provisioning now consists of following steps:

1. Create a dynamic provisioning profile
2. Create one or more provisioning rules
3. Associate a provisioning profile with a rule

Types of Dynamic Endpoint Provisioning Profiles

The RealPresence Resource Manager provides three types of provisioning profiles for use when you dynamically manage endpoints.

- **Network provisioning** profiles define network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on.

- **Admin Config** provisioning profiles define endpoint administrative settings such as maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on
- **Bundled provisioning** profiles allow you to configure endpoint system settings according to endpoint model and software version.

Dynamic Provisioning Profile	Former Name	Summary of Provisioned Settings:	How applied:
Network provisioning profile	Site provisioning profile	Network settings such as security, quality of service, and gatekeeper address, SIP server address, and so on.	Applied according to the provisioning rules you define.
Admin Config provisioning profile	User Group provisioning profile	Maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.	Applied according to the provisioning rules you define.
Bundled provisioning profile		Home screen settings related to user experience, monitor display and camera settings, password format settings and so on.	Applied according to model and software version of the particular endpoint.

Working with Provisioning Profiles

Navigate to **Endpoint > Dynamic Management > Provisioning Profiles** to work with both Network and Admin Config provisioning profiles.

See Using Bundled Provisioning Profiles on page 217 for detailed information about working with bundled provisioning profiles.

This section describes the following tasks:

- Create a New Provisioning Profile on page 182
- Edit a Provisioning Profile on page 182
- Reset a Default Provisioning Profile on page 183
- Edit a Default Provisioning Profile on page 183
- Reset a Provisioning Profile on page 184
- Clone a Provisioning Profile on page 184
- Delete a Provisioning Profile on page 184

For information on how to associate a profile with a provisioning rule, see Creating Dynamic Provisioning Rules on page 199.

Create a New Provisioning Profile

As soon as an endpoint is configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. So to ensure out-of-box usability, the RealPresence Resource Manager system comes with a default sprovisioning profiles. These default profiles cannot be customized with any rule. You need to create new provisioning profiles to customize network settings in your video environment.

New provisioning profiles are based on the default profiles and can be modified as much as needed. Any changes you make to the default profiles are not reflected in already-created profiles.

To create a provisioning profile

1 Go to **Endpoint > Dynamic Management > Provisioning Profiles**.

2 Click **Add**.

3 In the **General Info** section of the **Add New Profile** section, enter a name for the new provisioning profile.

4 Select a provisioning profile type from the drop-down list. Choose either a Network Provisioning Profile or an Admin Config Profile

5 As needed, edit the provisioning details and click **Apply**.

   For information about these network provisioning, see Available Settings for a Network Provisioning Profile on page 185.

   For information about Admin Config provisioning, see Available Settings for Admin Config Provisioning Profiles on page 195

6 Click **OK**.

Note

Not all of the provisioning parameters apply to all endpoint systems being provisioned. If an endpoint system does not have a corresponding parameter, it ignores the parameter.

Edit a Provisioning Profile

To edit an provisioning profile

1 Go to **Endpoint > Dynamic Managment > Provisioning Profiles**.

2 In the **Provisioning Profiles** page, select a profile and click **Edit**.

   For a detailed description of the endpoint fields you can configure when adding a new provisioning profile, see Available Settings for a Network Provisioning Profile on page 185 or Available Settings for Admin Config Provisioning Profiles on page 195.

   You may find more implementation details about these fields in the endpoint system documentation.

3 Click OK.

The provisioning profile is updated.

Reset a Default Provisioning Profile

You can reset the default profiles to their out-of-the-box values.

After you reset a default profile, the next time an endpoint is provisioned with the default profile, it will receive the new settings.

Default profiles are used for endpoints who do not meet the conditions of any provisioning rules.

To edit a default provisioning profile

1 Go to **Endpoint > Dynamic Managment > Provisioning Profiles**.

2 In the **Provisioning Profiles** page, select a default profile and click **Reset Default Profile**.

For a detailed description of the endpoint fields you can configure when adding a new provisioning profile, see Available Settings for a Network Provisioning Profile on page 185 or Available Settings for Admin Config Provisioning Profiles on page 195.

You may find more implementation details about these fields in the endpoint system documentation.

You cannot change the name of a default provisioning profile.

3 Click OK.

4 The default provisioning profile is updated.

Edit a Default Provisioning Profile

You can edit the default profiles to their out-of-the-box values.

To edit a default provisioning profile

1 Go to **Endpoint > Dynamic Managment > Provisioning Profiles**.

2 In the **Provisioning Profiles** page, select a default profile and click **Edit Default Profile**.

For a detailed description of the endpoint fields you can configure when adding a new provisioning profile, see Available Settings for a Network Provisioning Profile on page 185 or Available Settings for Admin Config Provisioning Profiles on page 195.

You may find more implementation details about these fields in the endpoint system documentation.

You cannot change the name of a default provisioning profile.

3 Click OK.

4 The default provisioning profile is updated.

Reset a Provisioning Profile

You can reset a provisioning profile you created to use the default values. When you reset a provisioning profiile it uses the values derived from the default template of the same type.

To reset a provisioning profile

1. Go to **Endpoint > Dynamic Managment > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select a default profile and click **Reset**.

   For a detailed description of the endpoint fields you can configure when adding a new provisioning profile, see Available Settings for a Network Provisioning Profile on page 185 or Available Settings for Admin Config Provisioning Profiles on page 195.

   You may find more implementation details about these fields in the endpoint system documentation.

   You cannot change the name of a default provisioning profile.
3. Click OK.

   The default provisioning profile is updated.

Clone a Provisioning Profile

To clone a provisioning profile

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

   The provisioning profile appears last in the Provisioning Profiles list.
4. As needed, edit the profile.

   See Edit a Provisioning Profile on page 182.

Delete a Provisioning Profile

To delete an provisioning profile

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

   The profile is deleted from the system.

Network Provisioning Profiles

With network provisioning profiles, you can ensure that all dynamically managed endpoints have the optimal and correct settings respective to their network location. For more information about dynamic endpoint management, see Understanding Dynamic Endpoint Management on page 156.

Network provisioning profiles allow you to provision endpoints with network settings such as security, quality of service, gatekeeper address, SIP server address, and so on.

As soon as an endpoint is configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. So to ensure out-of-box usability, the RealPresence Resource Manager system comes with a default Network provisioning Profile. This default profile cannot be associated with any rule.

You need to create new network provisioning profiles to have rule-based network settings in your video environment.

For information about how to add an Network provisioning profile, see Create a New Provisioning Profile on page 182.

Available Settings for a Network Provisioning Profile

Field	For the endpoint systems being provisioned...
Date and Time Settings	
Country	Specify the country code for their location.
Date Format	Specify the date display format.
Auto Adjust for Daylight Saving Time	Specify whether or not to adjust the endpoint’s system clock for daylight savings time.
Time Format	Specify the time display format.
Time Server	Specify whether to connect to a time server for automatic system time settings. Select **Auto** to require that the video endpoint system synchronize with an external time server that is identified by a network domain controller. Because it is identified by a network domain controller, you do not need to enter the IP address of the time server. Select **Manual** to require that the video endpoint system synchronize with an external time server that may not be identified by a network domain controller. In this case, you must also enter the IP address of the time server in the **Time Server Address** field. If **Time Server** is set to **Off**, or if the **Time Server** is set to **Manual** or **Auto** but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.
Primary Time Server Address	Specify the address of the primary time server when **Time Server** is set to **Manual**.
Secondary Time Server Address	Specify the address of the secondary time server when **Time Server** is set to **Manual**.

Field	For the endpoint systems being provisioned...
Timezone	Specify the time difference between GMT (Greenwich Mean Time) and the endpoint system’s location.
Firewall Settings	
Use Fixed Ports	Specify whether to define the TCP and UDP ports. • If the firewall is H.323 compatible or the endpoint systems are not behind a firewall, disable this setting. • If the firewall is not H.323 compatible, enable this setting. The endpoint systems will assign a range of ports starting with the TCP and UDP ports you specify. The endpoint system defaults to a range beginning with port 3230 for both TCP and UDP. **Note** You must open the corresponding ports in the firewall. You must also open the firewall’s TCP port 1720 to allow H.323 traffic.
Start TCP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify. **Note** You must also open the firewall’s TCP port 1720 to allow H.323 traffic.
Start UDP Port	Lets you specify the beginning value for the range of TCP ports used by the endpoint systems. The endpoint systems will automatically assign a range of ports starting with the port you specify.
Enable H.460 Firewall Traversal	Allows the endpoint system to use H.460-based firewall traversal. For more information, see the *Administrator’s Guide for Polycom HDX Systems*.
NAT Configuration	Specify 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**, specify the address that callers from outside the LAN should use to call the endpoint systems.
NAT is H.323 Compatible	Specify that the endpoint systems are behind a NAT that is capable of translating H.323 traffic.
Address Displayed in Global Directory	Specify whether to include the endpoint system’s information in the global directory • Select **Private** to exclude the endpoint from the global directory • Select **Public** to include the endpoint in the global directory
Enable SIP Keep Alives	When checked, SIP Keep Alive messages are enabled.

Field	For the endpoint systems being provisioned...
H323 Settings	
Enable IP H.323	Specify whether to enable IP H.323 calls.
Gatekeeper Address	When **Enable IP H.323** is set to **Specify**, enter the gatekeeper address. **Notes for endpoints that will use a RealPresence Access Director system or Polycom VBP** If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system or Polycom VBP system, the gatekeeper IP address should be the external or subscriber IP address of the RealPresence Access Director or Polycom VBP system.
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.
SIP Settings	
Enable SIP	Specify whether to enable SIP calls and enable the provisioning of SIP settings.
Automatically Discover SIP Servers	The RealPresence Resource Manager system will issue a DNS query to locate the SIP server and provision that information to endpoints.
Proxy Server	Specify the IP address or DNS name of the SIP proxy server for the network. **Notes for endpoints that will use a RealPresence Access Director system** If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system, the Proxy Server IP address should be the external or subscriber IP address of the RealPresence Access Director.
Registrar Server	Specify the IP address or DNS name of the SIP registrar server for the network. • In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server. • If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role. **Notes for endpoints that will use a RealPresence Access Director system** If this network provisioning profile is used for endpoints within a site that includes a RealPresence Access Director system, the Registrar Server address should be the external or subscriber IP address of the RealPresence Access Director.
Backup Proxy Server	Specify the IP address or DNS name of a backup SIP proxy server for the network. **Notes for endpoints that will use a RealPresence Access Director system** If this network provisioning profile is used for a endpoints within that includes a RealPresence Access Director system, the Backup Proxy Server IP address should be the IP address of the RealPresence Access Director.

Field	For the endpoint systems being provisioned...
Backup Registrar Server	Specify the IP address or DNS name of a backup SIP registrar server for the network. **Notes for endpoints that will use a RealPresence Access Director system** If this network provisioning profile is used for a site that includes a RealPresence Access Director system, the Backup Registrar Server IP address should be the IP address of the RealPresence Access Director.
Transport Protocol	Indicates the protocol the 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. • TCP provides reliable transport via TCP for SIP signaling. • UDP provides best-effort transport via UDP for SIP signaling. • TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.
SIP Server Type	Specify the type of the SIP registrar server. You can provision the following SIP registrar servers: • Standard (Polycom DMA system) • BroadSoft (BroadWorks) • Cisco (Cisco Unified Communications Manager) • Avaya (Avaya Communications Manager) • Siemens (OpenScape UC Server) • Microsoft (Lync of Office Communications Server)
Verify Certificate	Enable this option when the endpoint system's certificate should be verified by the certificate authority.
Use Endpoint Provisioning Credentials	Enable this option when the endpoint system should use the credentials the user entered at the endpoint for authenticating when registering with a SIP registrar server.
Use Enterprise URI	Enable this option with the endpoint should use the SIP URI of the enterprise user (domain user).
Common SIP User Name	Specify the name to use for authentication when registering with a SIP registrar server, for example, `msmith@company.com`. If the SIP proxy requires authentication, this field and the password cannot be blank. Common SIP credentials (username and password) can be used when the SIP server does not require unique user credentials.
Common SIP Password	Specify the password that authenticates the system to the registrar server. Common SIP credentials (username and password) can be used when the SIP server does not require unique user credentials.
Provisioning Settings	

Field	For the endpoint systems being provisioned...
Provisioning Polling Interval (minutes)	Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for new provisioning information. By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced.
Software Update Polling Interval (minutes)	Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for a new software update package. By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes.
Quality of Service Settings	
Video Type of Service Value	Specify the IP Precedence or Diffserv value for video packets.
Audio Type of Service Value	Specify the IP Precedence or Diffserv value for audio packets.
FECC Type of Service Value	Specify the IP Precedence or Diffserv value for Far End Camera Control packets.
Type of Service Field	Specify the service type and the priority of IP packets sent to the system for video, audio, and far-end camera control: • **IP Precedenc**e — Represents the priority of IP packets sent to the system. The value can be between 0 and 5. • **DiffServ** — Represents a priority level between 0 and 63. If this setting is selected, enter the value in the Type of Service Value field.
Maximum Transmission Unit Size (bytes)	Specify the Maximum Transmission Unit (MTU) size used in IP calls. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead, packets may be too small; increase the MTU.
Enable PVEC	Allows the endpoint system to use PVEC (Polycom Video Error Concealment) if packet loss occurs. PVEC delivers smooth, clear video over IP networks by concealing the deteriorating effects of packet loss
Enable RSVP	Allows the endpoint system to use Resource Reservation Setup Protocol (RSVP) to request that routers reserve bandwidth along an IP connection path. Both the near site and far site must support RSVP in order for reservation requests to be made to routers on the connection path.
Enable Dynamic Bandwidth	Specify whether to let the endpoint system automatically find the optimum line speed for a call.
Maximum Transmit Bandwidth (Kbps)	Specify the maximum transmission line speed.
Maximum Receive Bandwidth (Kbps)	Specify the maximum reception line speed.

Field	For the endpoint systems being provisioned...
Operation and Management Type	
Security Settings	
Security Profile	Read-only field. Displays the security level of the endpoint.
Use Room Password for Remote Access	Specify whether the local endpoint system password and remote access password are the same.
Room Password	Enter or change the local endpoint system password here. When the local password is set, you must enter it to configure the system Admin Settings using the remote control. The local password must not contain spaces.
Administrator ID	Enter the administrative account that should be used to access the endpoint system remotely.
Remote Access Password	For endpoint systems, enter or change the remote access password here. When the remote access password is set, you must enter it to upgrade the software or manage the endpoint systems from a computer. The remote access password cannot include spaces.
Meeting Password	Specify the password users must supply to join multipoint calls on this endpoint system if the call uses the internal multipoint option, rather than a bridge. This field can also be used to store a password required by another endpoint system that this system calls. If a password is stored in this field, you do not need to enter it at the time of the call; the endpoint system supplies it to the system that requires it. The meeting password cannot include spaces.
Enable Web Access	Specify whether to allow remote access to the endpoint system by the web. **Note** The endpoint systems will restart if the remote access settings are changed. This setting does not deactivate the associated port, only the application. Use the **Web Access Port** setting to disable the port.
Enable Secure Mode	Mark this check box to enable secure mode for the endpoints. If using secure mode, be sure your certificate set up is appropriate.
Enable AES Encryption	Select an AES Encryption mode: **Off**, **When Available**, **Required for Video calls,** or **Required for All Calls**.
Enable HTTPS only	Mark this check box to allow the endpoint to connect only using HTTPS.
Enable Telnet Access	Specify 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.

Field	For the endpoint systems being provisioned...
Web Access Port	Specify 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	Specify 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.
NTLM Version	Specify the NTLM version the endpoint system should use to authenticate.
Security Settings 2	
Idle Session Timeout in Minutes	When sessions are enabled, Specify the number of minutes your system can be idle before the session times out.
Lock Port after Failed Logins	Specify the number of failed login attempts allowed before the system locks the account. If set to Off, the system will not lock the user account due to failed login attempts. This selection controls local and web interface login attempts. For example, if you select 3 here, a user who fails to log in properly twice on the web interface and twice on the local interface is locked out on the fourth attempt.
Failed Login Window in Hours	Specify the amount of time that the account remains locked due to failed login attempts.
Port Lock Duration in Minutes	Specify the amount of time that the port remains locked due to failed login attempts.
Maximum Peer Certificate Chain Depth	Specify how many links a certificate chain can have. The term peer certificate refers to any certificate sent by the far-end host to the HDX system when a network connection is being established between the two systems.
Verify Certificates for all Web Access	Specify whether the endpoint requires certificate validation to access the endpoint.
Enable NIDS	Enable Network Intrusion Detection messages.
FIPS 140 Mode	
Whitelist	
Enable Whitelist of IPs	When a whitelist is enabled, allows access to an endpoint's web interface only by those systems with an IP address that matches a pattern using regular expression notation.

Field	For the endpoint systems being provisioned...
Enter all IPs allowed to Connect via the web	Specify (by IP addresses using regular expression notation) which systems can access an endpoint's web interface. Addresses are matched by pattern, which means that you could allows IP address that you did not mean to allow. For example, if you entered an IP address of 15.1.2.111, all of the following results would match: • 15.1.2.111 • 15.182.1.11 • 15.1.252.111 If you want to allow a range of IP addresses, use the * wildcard instead. For example, enter 10.11.*.* to allow all IP addresses that begin with 10.11.
General Settings	
Heartbeat Posting Interval (minutes)	Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for a heartbeat.
In Call Stats Posting Interval (minutes)	Specify the frequency at which the endpoint systems poll the RealPresence Resource Manager system for in call statistics.
Calendaring Settings	
Automatically Discover Exchange Server	Specify that the RealPresence Resource Manager system should discover the Microsoft Exchange server for the site by searching DNS records.
Specify Exchange Server	Specify that the RealPresence Resource Manager system should use the Microsoft Exchange server specified in the Exchange Server Address field.
Exchange Server Address	Specify the IP address or DNS name of the Microsoft Exchange server for the site.
Enterprise Directory Settings	
Group Display Name	Specify whether the RealPresence Resource Manager system should identify groups by their common name (cn) or their DisplayName. These names are extracted from the Active Directory.
User Display Name	Specify whether the RealPresence Resource Manager system should identify users by their common name (cn) or their DisplayName. These names are extracted from the Active Directory.
Enterprise Directory Admin Group	Specify the Active Directory group whose members should have access to the Admin settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed.
Enterprise Directory User Group	Specify the Active Directory group whose members should have access to the User settings on the HDX system. This name must exactly match the name in the Active Directory server for authentication to succeed.
Directory Settings	
Use Default Directory Server	

Field	For the endpoint systems being provisioned...
Specify	When the **Use Default Directory Server** radio button is marked, you can use the **Directory Server** field enter the IP address of the directory server you wish to use.
Verify Certificate	
Presence Settings	
Use Default Presence Server	
Presence Server	When the Use Default Presence Server button is marked, you can use the **Presence Server** field enter the IP address of the presence server you wish to use.
Verify Certificate	
SNMP Settings	
Enable SNMP Access	Specify whether to allow remote acces to the system by SNMP. **Note** The endpoint 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.
SNMP Version1	Mark to enable SNMP Version1.
SNMP Version2C	Mark to enable SNMP Version2C.
SNMP Version3	Mark to enable SNMP Version3.
Transport Protocol	Select TCP or UDP.
Listening Port	The default port is 161.
Read-only community	
Contact Name	
Location Name	
User Name	
Auth Algorithm	
Auth Password	
Privacy Algorithm	
Privacy Password	
Notification Receiver 1	Enter the following information: **Server Address** **SNMP Version** **Listening Port** **Trap/Inform**

Field	For the endpoint systems being provisioned...
Notification Reciever 2	Enter the following information: **Server Address** **SNMP Version** **Listening Port** **Trap/Inform**
Notification Receiver 3	Enter the following information: **Server Address** **SNMP Version** **Listening Port** **Trap/Inform**

Admin Config Provisioning Profiles

Admin Config provisioning profiles, allow you to create provisioning profiles that include maximum and preferred call speeds for H.323 settings, calendaring settings, Microsoft Lync settings, and so on.

You can use Admin Config provisioning profiles to provision the following Polycom endpoints:

- Polycom VVX systems deployed in dynamic management mode
- Polycom HDX systems deployed in dynamic management mode
- Polycom RealPresence Group Series endpoints (required)
- Polycom RealPresence Immersive Studio systems (required)
- Polycom CMA Desktop clients
- RealPresence Mobile clients
- RealPresence Desktop clients

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

As soon as an endpoint is configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. So to ensure out-of-box usability, the RealPresence Resource Manager system comes with a default Admin Config provisioning Profile. This default profile cannot be customized with any rule. You need to create new Admin Config provisioning profiles to customize endpoint configuration settings in your video environment.

- If an Admin Config provisioning profile provisions a setting that the endpoint is not capable of fulfilling, the endpoint will ignore those settings.
- The name of the Default Provisioning Profile is stored in the system database and is not localized into other languages. You cannot change the name.

For information about how to add an Admin Config provisioning profile, see Create a New Provisioning Profile on page 182.

Available Settings for Admin Config Provisioning Profiles

The following table shows the fields you can configure when adding a new Admin Config provisioning profile to the Polycom® RealPresence® Resource Manager system. You may find more implementation details about these fields in the endpoint system documentation.

To view these fields, go to **Endpoint > Dynamic Management > Provisioning Profiles**. Then choose **Add** and choose **Admin Config Provisioning Profile**.

Field	For the endpoint systems being provisioned...
System Settings	
Language	Specifies the language for the video endpoint system's user interface. Possible values include: Arabic, Simplified Chinese, Traditional Chinese, English_US, English_UK, French, German, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, and Spanish.
Allow Access to User Setup	Specifies whether the **User Settings** screen is accessible to users via the **System** screen. Select this option to allow endpoint system users to change limited environmental settings.
Allow Directory Changes	Specifies whether endpoint system users can save changes they make to the directory on contacts/favorites list.
Auto-answer Point to Point Calls	
Auto-answer Multipoint calls	
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 will not be able to retrieve Call Detail Report (CDR) records.
Maximum Time in Call (minutes)	Specifies the maximum number of minutes allowed for a call. Enter 0 to remove any limit.
Recent Calls	Specifies whether to display the **Recent Calls** button on the home screen. The **Recent Calls** screen lists the site number or name, the date and time, and whether the call was incoming or outgoing. **Note** If the **Call Detail Report** option is not selected, the **Recent Calls** option is not available.

Field	For the endpoint systems being provisioned...
Screen Saver Wait Time	Specifies how long the system remains awake during periods of inactivity. The default is 3 minutes. If the system requires users to log in, the screen saver timeout also logs out the current user. Setting this option to **Off** prevents the system from going to sleep. To prevent image burn-in, specify 15 minutes or less.
Directory Search Mode	Specifies how endpoint directory searches are initiated by the endpoint user. Possible values are: • Auto—The search is executed after the user stops entering characters. • Manual—The search is executed only when the user explicitly clicks the **Search** button.
Maximum Number of Active Web Sessions	Specifies the number of active web sessions that are allowed. The default is **25**.
Home Screen Settings	
Display H.323 Extension	Lets users placing a gateway call enter the H.323 extension separately from the gateway ID. If you do not select this setting, endpoint system users make gateway calls by entering the call information in this format: `gateway ID + ## + extension`
Enable Availability Control	When enabled, lets users set their availability in the endpoint system's local user interface.
H.323 Settings	
Maximum Speed for Receiving Calls (kbps)	Allows you to restrict the bandwidth used when receiving calls. If the far site attempts to call the endpoint system at a higher speed than selected here, the call is re-negotiated at the speed specified in this field. The default is **384** kbps.
Preferred Speed for Placing Calls (kbps)	Determines the speeds that will be used for calls from this endpoint system when: • The **Call Quality** selection is either unavailable or set to **Auto** on the **Place a Call** screen • The call is placed from the directory If the far-site endpoint system does not support the selected speed, the endpoint system automatically negotiates a lower speed. The default is **384** kbps.
Call Settings	
Preferred Dialing Method	Specifies the preferred method for dialing various call types. • If set to **Auto** (default), calls use the configured dialing order. • If set to **Manual**, the endpoint systems will prompt the user to select the call type from a list when placing a call.

Field	For the endpoint systems being provisioned...
Audio Settings	
Mute Auto Answer Calls	Specifies whether or not to automatically mute incoming calls. The default setting is to **not** automatically mute incoming calls.
Software Endpoint Settings	
Enable IM/Chat	For RealPresence Desktop clients, this option must be provisioned to support both presence and chat functions. For CMA Desktop, this option must be provisioned to support chat functions.
Enable Screen Saver When in Call	
Auto Accept Invitation	Enables the client to auto-accept chat invitations. Applicable to RealPresence Desktop clients only.
Allow IM Storage	Allows the client to store chat history on its local drive. Note: If you disable this option after enabling it, all chat history is cleared for the client. Applicable to RealPresence Desktop clients only.
Provision Check that the CMA Desktop is the default program for:	• Opening Call To links • Opening H323 links • Opening SIP links Marking this setting provisions the CMA Desktop to be the default program for opening the above links.
Provision Enable Sending 720p (HD) Video	Mark this check box to enable sending HD video. This is enabled by default.
Allow 720p frame rates up to:	Enabled when Provision Enable Sending 720p (HD) people video is also marked. You can choose 15 Frames per second or 30 Frames per second.
Calendaring Settings	
Enable Calendaring	When enabled, specifies that the Resource Manager system will provision the endpoint for Polycom Conferencing for Outlook. This includes provisioning the Microsoft Exchange server and calendaring settings for the endpoint system.
Alert Tone	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.
Display Private Meeting	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.
Meeting Reminder Time	Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.

Field	For the endpoint systems being provisioned...
Microsoft Lync Settings	
Group Name	Specifies the group name for which the endpoint system should be provisioned.
VVX Settings	
Configuration Server URL	Specifies the IP address for the system that will provide provisioning service. All addresses can be followed by an optional directory and optional filename.
Logging Server URL	Specifies the directory to use for log files, if required. A URL can also be specified. This field is blank by default.
Configuration Data	Enter XML data for a custom configuration. Allows the Resource Manager system administrator's to provision settings that the Resource Manager system does not normally provide.

Creating Dynamic Provisioning Rules

You apply dynamic provisioning profiles by using RealPresence Resource Manager system's rule-based system. You can create multiple rules and associate a profile with more than one rule at a time. A provisioning rule consists of one or more conditions that must be met before the dynamic provisioning profile can be applied.

For example, you can use provisioning rules to provision different endpoints within the same site with different network settings.

If a dynamically-managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

This chapter describes RealPresence Resource Manager system provisioning rules operations. It includes these topics:

Activating Provisioning Rules

Provisioning rules must be activated in order for them to be used in dynamic provisioning.

When you create a rule, it is activated by default and will be used the next time a polling endpoint or server meets the conditions of the rule.

If you want to change a rule, you must de-activate it before you can edit it. If you want to stop using a provisioning rule, you need de-activate it. In addition, you cannot delete an activated provisioning rule.

Prioritizing Provisioning Rules

After you have added more than one provisioning rule, you can change the priority of the list of provisioning rules you created. When you add rules, they are automatically prioritized according to the order in which they were added to the system.

Rules with a higher priority will be applied first. The Priority determines which provisioning rule takes priority.

Consider the following example:

Create two rules, one for the Support user group and one for the Toronto user group. Jason Smith is part of the Support group and also part of the Toronto group.

- The Support Rule is assigned an Admin Config provisioning profile named Low-Bandwidth, which allows a maximum speed for receiving calls of 128kbps. The Support Rule is assigned a priority of 1.
- The Toronto Rule is assigned a Admin Config provisioning profile called High-Bandwidth, which allows a maximum speed for receiving calls of 1920kbps. The Toronto Rule is assigned a priority of 2.

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

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

Using Rule Conditions

A provisioning rule is comprised of one or more conditions that you define. RealPresence Resource Manager system allows you to define four types of conditions: site, user group, user, and device.

You are allowed add to multiple conditions of multiple condition types to a single rule.

For example, you can create a rule that applies a provisioning profile according to the user group (condition) and device type (condition).

Rule conditions can be complex and include OR or AND operations, as well as NOT conditions.

If a dynamically-managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

For example, you can create a rule that applies a network provisioning profile for all device types within a site except for VVX endpoints.

See Working with Provisioning Rules on page 201.

Working with Provisioning Rules

When you create a provisioning rule, you can associate multiple profile types with the same provisioning rule. For example, when you provision an RealPresence Access Director for your environment, it is typical to associate a Network provisioning profile, an Admin Config provisioning profile, and an RPAD server provisioning profile with the same rule.

If a dynamically-managed endpoint does not meet any conditions of any rule, it is provisioned with the default profiles.

This topic describes the provisioning rule operations a user assigned the Administrator role can perform.

These are:

- Add a Provisioning Rule on page 202
- Edit the Priority of a Provisioning Rule on page 205
- Clone a Provisioning Rule on page 206

- De-activating a Provisioning Rule on page 206
- Edit a Provisioning Rule on page 206
- Delete a Provisioning Rule on page 207

Add a Provisioning Rule

This topic describes how to add provisioning rules. Only users with the administrator role can add provisioning rules.

> Add new provisioning rules in the middle of the work day, not first thing in the morning.

When you add a new provisioning rule or change its priority, the RealPresence Resource Manager system immediately rolls it out. If it rolls it out first thing in the morning, people who need to attend a “start the day” conference will have to first wait for their endpoint to be provisioned. Polycom recommends implementing profiles in the middle of the work day and then let the provisioning occur at the designated polling interval.

When you add a provisioning rule, you use the **Add New Rule** dialog box to complete the following steps:

1. Name the Provisioning Rule.
2. Activate the Rule.
3. Add a condition(s) to a provisioning rule.
4. Associate Provisioning Profiles with a Provisioning Rule.

The following steps incorporate an example of creating a rule that applies provisioning profile to all devices of a certain type within a specific site. You can create rules of varying complexity or simplicity. The following is just one example.

See Using Rule Conditions on page 200 for other examples.

Name the Provisioning Rule

Each provisioning rule you create must have a unique name as well as a description.

To create and name a provisioning rule

1. Navigate to **Endpoint > Dynamic Management > Provisioning Rules.**
2. Click **Add**.

   The **Add New Rule** dialog box displays.
3. In the **General Info** area, enter a name for the new rule.

   In this example, we are creating a rule for all HDX systems in the Austin, Texas.

   Next you will ensure that the provisioning rule is active, if needed. Do not close the dialog box.

Activate the Rule

By default, a rule is marked as active when you create it. Active rules are automatically sent the next time a dynamically-managed device polls the RealPresence Resource Manager system for provisioning updates.

If you do not want the rule to be active, unmark the Active check box.

The next step is to add one or more conditions to your rule. Do not close the dialog box.

Add a condition(s) to a provisioning rule

You can add condition to a provisioning rule when you first create it or you can add a new condition or change a condition of an inactive rule.

Rules are comprised of one or more conditions. The RealPresence Resource Manager system supports the following condition types:

Condition Type	Attributes
Site	The site name.
User Group	The name of a user group.
User	You can choose from one of the following user attributes when defining a user condition for a rule: • Title • Department • User ID
Device	You can choose from the following attributes when defining a device condition for a rule: • Device Type • Serial Number

To add a condition to a provisioning rule

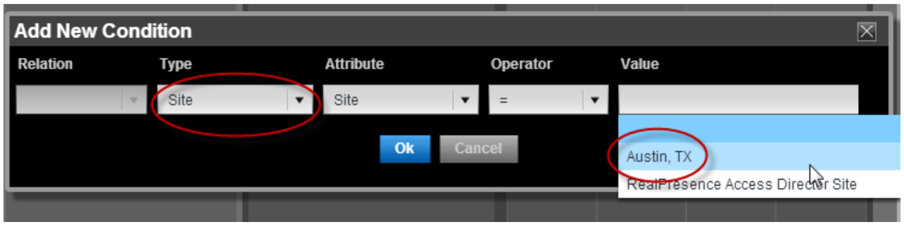
1 In the Add New Rule dialog box, click the **Add** button in the **Condition** area.

The **Add New Condition** dialog box displays.

2 Use the **Add New Condition** dialog box to create the conditions that you need.

a Select a condition **Type.**

In this example, we are creating a condition for the Austin site, we chose the site **Type**, and selected the Austin site for the **Value**.



Relation	Type	Attribute	Operator	Value
	Site	Site	=	

Austin, TX
RealPresence Access Director Site

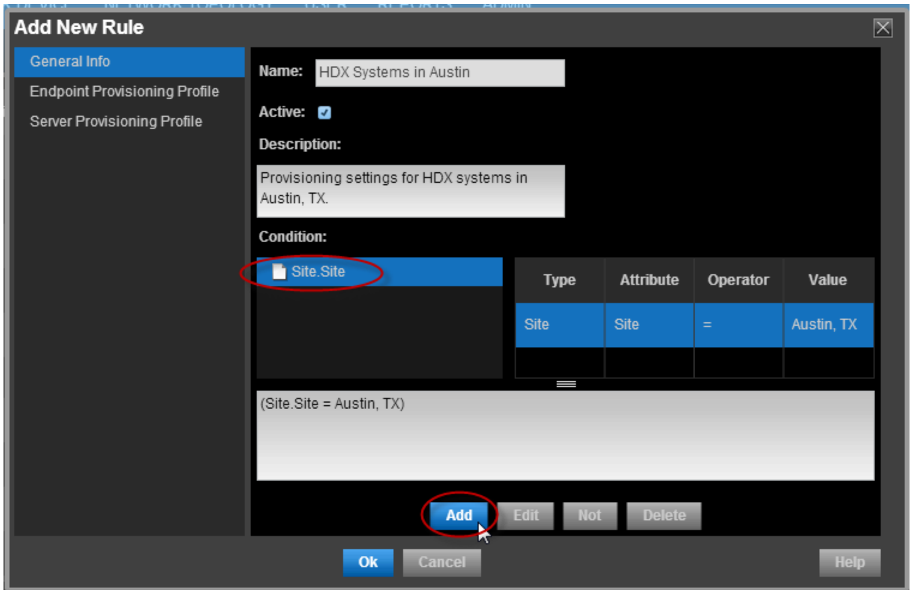
b Click **Ok** to save the condition.

In our example, we are going to define a condition for the rule to include all HDX systems.

c To add another condition, first select the condition you just created and then click **Add**.

To add a new condition to a rule, you must select a condition on the list from which to build on.

In this example, we have selected the Site condition created in the previous step. When we selected the Site condition, we can then click **Add** button to add more conditions to our rule.



Name: HDX Systems in Austin

Active: ☑

Description:

Provisioning settings for HDX systems in Austin, TX.

Condition:

Site.Site

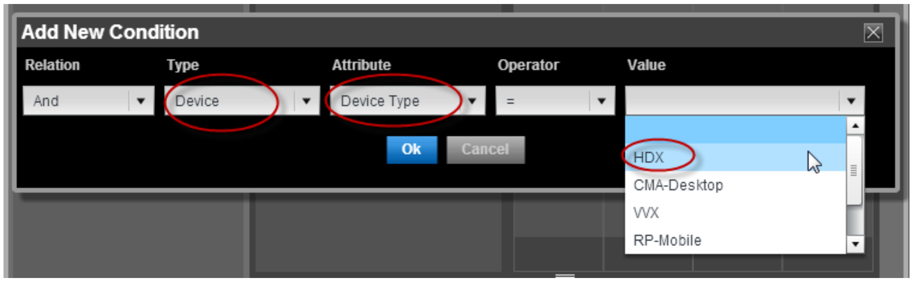
Type	Attribute	Operator	Value
Site	Site	=	Austin, TX

(Site.Site = Austin, TX)

d Select a value from the **Relation** column. You can relate multiple conditions with an **And** statement or an **Or** statement.

In our example, we want this rule to apply to both the site and the device type, so we chose **And**.

This screenshot shows a Device condition type that defines a condition that includes all HDX device types.



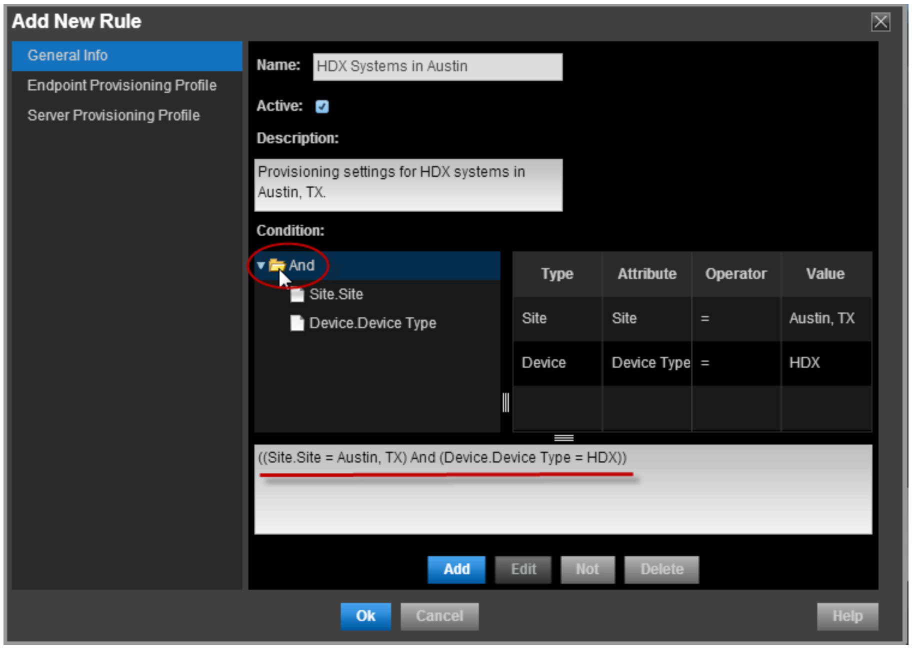
Add New Condition

Relation	Type	Attribute	Operator	Value
And	Device	Device Type	=	

e Click **Ok** to save the condition.

f To view all conditions in your rule, expand the folder.

In our example, we expanded the **And** folder to view each condition. Notice that the condition is also displayed.



Add New Rule

Name: HDX Systems in Austin

Active: ☑

Description:

Provisioning settings for HDX systems in Austin, TX.

Condition:

Type	Attribute	Operator	Value
Site	Site	=	Austin, TX
Device	Device Type	=	HDX

((Site.Site = Austin, TX) And (Device.Device Type = HDX))

The next step in the **Add New Rule** dialog is to associate provisioning profiles with the rule. Do not close the **Add New Rule** dialog box.

Associate Provisioning Profiles with a Provisioning Rule

After you have created your condition(s), you need to select which provisioning profiles to associate with this rule. You must have already created the provisioning profiles you need.

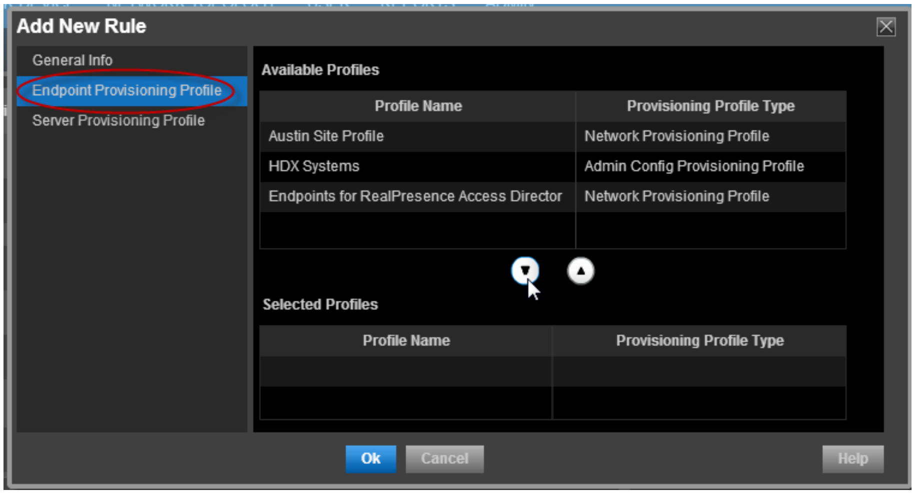
A provisioning rule must have at least one profile associated with the rule.

See Using Provisioning Profiles on page 180.

To associate provisioning profiles with your rule

1 To associate an endpoint provisioning profile such as a Network Provisioning profile or Admin Config profiile, navigate to the **Endpoint Provisioning Profile** page in the **Add New Rule** dialog box.

You can associate more than one profile to the rule. Although, you can only associate one profile of any particular type. For example, one Network Provisioning Profile, one Admin Config Profile, and one Server Provisioning profile.



Available Profiles

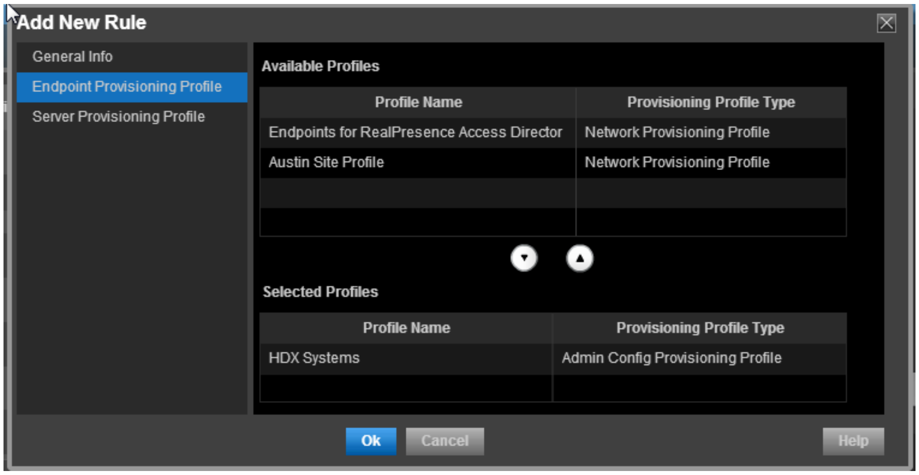
Profile Name	Provisioning Profile Type
Austin Site Profile	Network Provisioning Profile
HDX Systems	Admin Config Provisioning Profile
Endpoints for RealPresence Access Director	Network Provisioning Profile

Selected Profiles

Profile Name	Provisioning Profile Type

2 Select the **Available Profiles** you want to associate with the rule you created and click the down arrow to move them to the **Selected Profiles** section.

In this example, we selected the HDX Systems profile which is an **Admin Config** provisioning profile that was created for this example.



Available Profiles

Profile Name	Provisioning Profile Type
Endpoints for RealPresence Access Director	Network Provisioning Profile
Austin Site Profile	Network Provisioning Profile

Selected Profiles

Profile Name	Provisioning Profile Type
HDX Systems	Admin Config Provisioning Profile

3 You have now finished creating a provisioning rule. Click **Ok** to save the rule.

These steps used an example rule that applied the associated profile to all HDX systems within a example Austin site.

Edit the Priority of a Provisioning Rule

By default, provisioning rules are assigned a priority level according to order in which they added to the system. You can raise the priority of a provisioning rule.

Provisioning rules with higher priority get applied first.

To edit the priority of a provisioning rule

1 Go to **Endpoint > Dynamic Managment> Provisioning Rules**.

2 In the **Provisioning Rules** page, select the profile of which you want to increase the priority.

3 Click **Priority Up** or **Priority Down**.

The system raises or lowers the priority of the selected provisioning rule.

Clone a Provisioning Rule

You can clone a provisioning rule when you want to re-use most of its conditions in a new rule or just change the name of an existing rule.

To clone a provisioning rule

1 Go to **Endpoint > Dynamic Management > Provisioning Rules**.

2 In the **Provisioning Rules** page, select the rule you want to clone and click Clone.

3 In the **Clone Rule** dialog box, enter a name for the new rule and click Save.

The provisioning rule appears last in the **Provisioning Rules** list.

4 As needed, edit the rule.

De-activating a Provisioning Rule

You can de-activate a provisioning rule if you want to stop using it as a provisioning rule or edit it. De-activated provisioning rules are not used.

You must activate a provisioning rule for it to be used.

To de-activate a provisioning rule

1 Navigate to **Endpoint > Dynamic Managment > Provisioning Rule**.

2 In the **Provisioning Rule** page, select the rule and click Deactivate.

3 Click **Yes** to confirm the de-activation.

Edit a Provisioning Rule

You cannot edit an active provisioning rule. You must first de-activate it before you can make any changes.

To edit a provisioning rule

1. Go to **Endpoint > Dynamic Managment > Provisioning Rule**.
2. In the **Provisioning Rule** page, select the rule and click Deactivate.
3. Click **Yes** to confirm the de-activation.
4. Select the rule you de-activated and click **Edit**.

   For a detailed description of how to create a rule, seeAdd a Provisioning Rule on page 202 .
5. Click OK.

   The provisioning rule is updated.

Delete a Provisioning Rule

You cannot delete an active provisioning rule. You must first de-activate it before you can delete it.

To delete an provisioning rule

1. Go to **Endpoint > Dynamic Management> Provisioning Rules**.
2. In the **Provisioning Profiles** page, select the profile and click De-Activate.
3. Click **Yes** to confirm the de-activation.
4. Select the de-activated rule and click **Delete**.
5. Click **Yes** to confirm the deletion.

   The rule is deleted from the system.

Dynamically Managing Endpoint Naming Schemes

The RealPresence Resource Manager allows administrators to configure their E.164 alias, system naming schemes and SIP URIs for endpoints that are dynamically managed.

If you choose to provision H.323 settings through a network provisioning profile, you can also define the E.164 number and system naming scheme used for endpoints. You can also auto-generate SIP URIs for dynamically-managed endpoints.

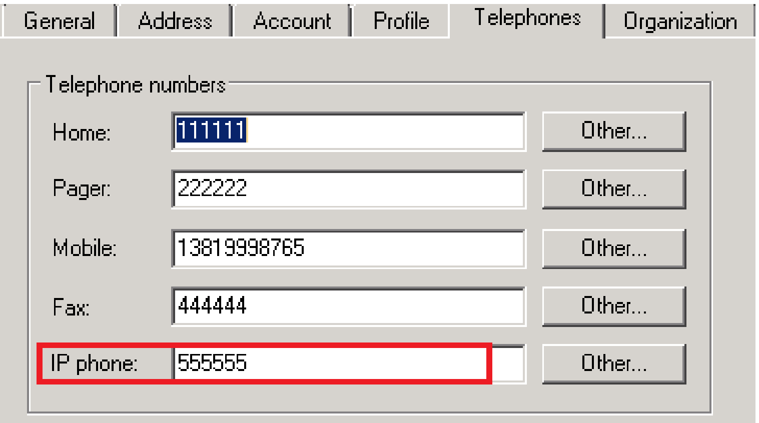
This section discusses these topics:

Using Custom Active Directory Attributes

When your system is integrated with Active Directory, RealPresence Resource Manager only incorporates and displays attributes from the Active Directory record that are part of the Active Directory Global Catalog. When you define E.164 numbers and SIP URIs, you can use Active Directory attributes that are not displayed in the RealPresence Resource Manager system user record.

For example, the below diagram displays some telephone numbers that can be configured in Active Directory. By default, when you integrate your RealPresence Resource Manager system with Active Directory only the default phone number field is used within the E.164 Numbering scheme..

If you wanted use the **IP Phone** attribute instead of the default phone number, you need to define that attribute name that in RealPresence Resource Manager system when you create a naming scheme.



Home: 111111

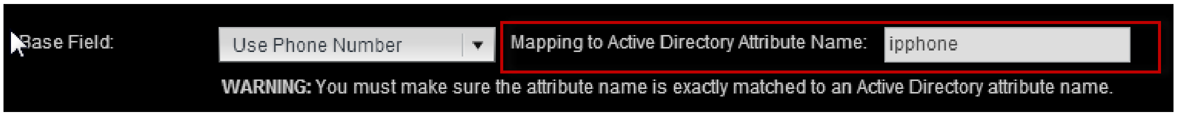
Pager: 222222

Mobile: 13819998765

Fax: 444444

IP phone: 555555

The following screenshot displays the IP Phone attribute being defined when you create an E.164 naming scheme:



Base Field: Use Phone Number

Mapping to Active Directory Attribute Name: ipphone

WARNING: You must make sure the attribute name is exactly matched to an Active Directory attribute name.

Notice that you must use the correct name of the attribute. In addition, the attribute that you want to use must be made available to the RealPresence Resource Manager system by being included in the Active Directory Global Service.

Active Directory Global Service

To take advantage of custom Active Directory attributes in RealPresence Resource Manager, your Active Directory administrator must ensure that the attributes you want to use have been added to the Active Directory Global Catalog service.

You must work with your Active Directory administrator to decide how to manipulate the Active Directory schema to ensure that the attributes you want to use in naming schemes are available to the RealPresence Resource Manager system.

The Active Directory global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

However, to minimize replication traffic and keep the global catalog's database small, only selected attributes of each object are replicated. This is called the partial attribute set (PAS). The PAS can be modified by modifying the schema and marking attributes for replication to the global catalog.

The Active Directory administrator can do this by ensuring that the corresponding attributes are included in the Partial Attribute Set. See http://support.microsoft.com/kb/248717 for information about "*How to Modify Attributes That Replicate to the Global Catalog*."

Define an E.164 Address Scheme

You can define an E.164 address scheme that will be used when provisioning E.164 addressed to all dynamically-managed endpoints.

You can choose to use to define a number range, use the default phone number or use a different Active Directory attributes. See Using Custom Active Directory Attributes on page 209.

To define an E.164 address scheme for dynamically-managed endpoints

1. Navigate to **Endpoint > Dynamic Management > E.164 Numbering**.
2. Define your numbering scheme according to the options provided.

   The administrator has the following options when implementing an E.164 numbering scheme:

Option	Usage
Select Area	When areas are enabled, you can select an area to which you want to apply this E.164 numbering scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage. Users with the administrator role can always select an area when areas are enabled.
Prefix	• **No Prefix**—The system will not append a prefix to create the E.164 assignment. • **A Number** —The system appends the prefix specified to create the E.164 assignment. • **Based on Device Type**—The system appends a Device Type prefix to create the E.164 assignment. You can use the suggested prefix or click the **Device Number** field to edit the prefix for the device type. This options is not available if you choose to use a suffix based on the device type.

Option	Usage
Base Field	**You can define a specific number range or indicate that a phone number be used for the Base Field:** To specify a **Number Range**: **1** In the **Base Field**, select Specify Number Range **2** Use the **To** and **From** fields to define the number range. To use a **Phone Number**: **1** In the **Base Field**, select **Use Phone Number**. **2** If you want to use the main phone number field from Active Directory, leave the Mapping to Active Directory Name field blank. **3** If you want to use a number other than the one indicated in the Phone Number field in Active Directory, you can indicate another Active Directory attribute to use. ⅄ For example, if your Active Directory also includes mobile number information in an Active Directory Attribute called `mobilenum`, you should select **Use Phone Number** and then enter the name `mobilenum` in the **Mapping to Active Directory Name** field. For more information on which Active Directory attributes can be used, see To auto-generate SIP URIs for dynamically-managed endpoints on page 215. **4** Enter the **Maximum number of digits to use** from the user's phone number (between 3 and 10 digits). The digits from the phone number are selected from right to left. **5** Enter **Number range to use if phone number is empty** (reverts to **Specify Number Range)**—The system will revert to using a number range if the user's phone number is empty.
Suffix	• **No Suffix**—The system will not append a suffix to create the E.164 assignment. • **A Number** —The system appends the suffix specified to create the E.164 assignment. • **Based on Device Type**—The system appends a pre-defined Device Type suffix to create the E.164 assignment. You can use the suggested suffix or click the Device Number field to edit the suffix for the device type. This option is not available if you used a prefix based on the device type.

> The total number of digits specified for an E.164 number must be 15 or less. If the user's phone number is used as the base field, the system reserves one digit to differentiate between the user's multiple devices. In this case the total number of digits configured cannot exceed 14 digits.

3 When finished defining your numbering scheme, click **Update**.

Settings are applied the next time the endpoint polls for a dynamic provisioning update.

Define a System Naming Scheme and H.323 Alias

You can define an system naming scheme that will be provisioned to all dynamically-managed endpoints.

When you define the system name, you can choose to have the system name also serve as the H.323 alias for the endpoint. This is the default.

Alternatively, you can use a different name for the H.323 alias and the system name and define a naming scheme for both.

To define a system naming scheme for dynamically-managed endpoints

1. Navigate to **Endpoint > Dynamic Management > System Naming**.
2. Build your system naming scheme.

   System names can be a combination of up to four naming fields and three separators. For example, the following system name is defined by selecting **UserID**, **City** and **Device Type** fields and by using two "**.**" separators: `UserID.City.HDX`.

   The administrator has the following options when implementing a system scheme:

Option	Usage
Select Area	When areas are enabled, you can select an area to which you want to apply this system naming scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage.

Option	Usage
Naming Field	The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme. • Last Name • First Name • User ID • City • Department • Device Type • Domain • Title • Area (only available when areas are enabled) You cannot use the same naming field more than once within the same naming scheme.
Separator	You can use a separator between each naming field. If you do not want to use a separator, you must select (none). Choose from the following separators: • (none) • (space) • , • - • _ You can use the same separator multiple times.

3. To use the system name as the hostname for hard endpoints (such as RealPresence Group Series, HDX, or RealPresence Immersive Studio systems), mark the **Use system name for hard endpoint hostname** check box.
4. To use same naming scheme for the H.323 alias, ensure that the **Use system naming for H323 ID** check box is marked.
5. To use a different naming scheme for the H.323 alias:
   a. Unmark the **Use system naming for H323 ID** check box.
   b. Build your H.323 ID scheme according to the same options as the System Name.

      The administrator has the following options for an H.323 ID scheme:

Option	Usage
Select Area	When areas are enabled, you can select an area to which you want to apply this system naming scheme. This field is only available to users who manage more than one area. The drop-down list lists only those areas that the user has permission to manage.
Naming Field	The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme. • Last Name • First Name • User ID • City • Department • Device Type • Device Model • Domain • Title • Area (only available when areas are enabled) You cannot use the same naming field more than once within the same naming scheme.
Separator	You can use a separator between each naming field. If you do not want to use a separator, you must select (none). Choose from the following separators: • (none) • - • _ You can use the same separator multiple times.

6 When finished, click **Update**.

Settings are applied the next time the endpoint polls for a dynamic provisioning update.

Auto-Generate SIP URIs for Dynamically-Managed Endpoints

You can automatically generate a SIP URI for each dynamically-managed endpoint according to a naming scheme you define.

You can choose to use the user email address as the SIP URI or define a custom URI from Active Directory attributes. See Using Custom Active Directory Attributes on page 209.

When you define a custom SIP URI from Active Directory fields, you can choose one of the default fields or an different Active Directory attribute.

To auto-generate SIP URIs for dynamically-managed endpoints

1 Navigate to **Endpoint > Dynamic Management > SIP URI**.

2 If areas are enabled, select an area from the **Select Area** drop-down list.

The **Select Area** drop-down list is available to users with the administrator or area administrator role. The areas included in the list are restricted to those areas that the user is allowed to manage.

3 Mark the **Auto-generate SIP URIs for all users** check box.

You can either use the user’s email address as the SIP URI or define the SIP URI yourself.

4 To use the user’s email address as their SIP URI. Check the **Use the user’s email address as their SIP URI** if you want this option.

If you choose this option, you cannot further define the fields used for the SIP URI.

5 To define a SIP URI, complete the naming fields and separators.

SIP URIs can be a combination of up to four naming fields, three separators and domain name suffix. For example, the following SIP URI is defined by selecting UserID, City and Device Type fields, by using two “.” separators and domain name "abc.com": UserID.City.HDX@abc.com.

You can use a pre-defined naming field from the drop-down list or type a specific Active Directory attribute.

a To use a pre-defined field, select it from the drop-down list. Pre-defined fields include: **Last Name**, **First Name**, **User ID**, **City**, **Department**, **Device Type**, **Device Model**, **Domain**, and **Title**.

b To use an Active Directory attribute, select **AD Attribute** from the drop-down list and enter the name of the attribute in the **Attribute Name** field. The attribute you enter must exactly match an existing Active Directory attribute. Talk to your Active Directory administrator if you have questions about which Active Directory attributes are available for use.

As a best practice, include be sure to include the **Domain** information in the SIP URI definition.

Option	Usage
Naming Field	The following fields are available to use as a naming field. Be sure that the field you choose is populated for all users in your system. You cannot use the same naming field twice in the same scheme. • Last Name • First Name • User ID • City • Department • Device Type • Device Model • Domain • Title • AD Attribute. ➤ When you select AD attribute, you must also enter an name in the **Attribute Name** field. The name must match an available Active Directory attribute. You cannot use the same naming field more than once within the same naming scheme.
Separator	You can use a separator between each naming field. If you do not want to use a separator, you must select (none). Choose from the following separators: • (none) • . • - • _ • @ • You cannot use the @ separator more than once and it cannot be used before the _ separator.
Domain name suffix	Adds the domain suffix to the naming field you choose. You can either choose None or select “A String (specify) to enter the domain suffix as a string value. For example, LastName.FirstName@domainsuffix.com can be defined by selecting LastName and FirstName as naming fields with a . separator. The Domain suffix in this example was entered as a string.

6 Mark the **Keep URIs Unique** check box if you want unique SIP URIs for each endpoint regardless of user.

If you leave this check box unmarked, the user’s SIP URI can be used for each endpoint associated with that user.

7 Click **Update**.

Using Bundled Provisioning Profiles

The Polycom® RealPresence® Resource Manager system supports **Bundled Provisioning Profiles** for dynamically managed Polycom RealPresence Group systems, Polycom RealPresence Immersive Studio systems and Polycom HDX (v3.0.3 and higher) systems. With **Bundled Provisioning Profiles**, a RealPresence Resource Manager user with the administrator role can download a bundled provisioning profile from any already configured HDX or RealPresence Group system that is dynamically managed by the RealPresence Resource Manager.

You can then indicate which dynamically managed Polycom HDX or RealPresence Group system(s) of the same model and software version will receive the bundled provisioning profile when it next polls the RealPresence Resource Manager system for new provisioning information.

> Some configuration settings on dynamically managed endpoints that the RealPresence Resource Manager system provisions are associated with the site where the endpoint system is located.

Bundled provisioning profiles provides businesses with an efficient and effective way to provision RealPresence Group systems, RealPresence Immersive Studio systems, and ReaPolycom HDX systems consistently across each model. Endpoint users with administrative rights can still change the settings on an HDX system after the bundled provisioning profile is applied. However, if another profile is sent by the RealPresence Resource Manager system, it will overwrite the user’s changes.

This chapter describes how to work with bundled provisioning profiles. It includes these topics:

- Provisioning Best Practices
- How Bundled Provisioning Works on page 218
- Download a Bundled Provisioning Profile on page 218
- View the List of Bundled Provisioning Profiles on page 219
- Edit a Bundled Provisioning Profile on page 220
- Re-associate Devices with a Different Profile on page 221
- Delete a Bundled Provisioning Profile on page 221
- Settings included in a Bundled Provisioning Profile for an HDX on page 222
- Settings included in a Bundled Provisioning Profile for a RealPresence Group System and RealPresence Immersive Studio System on page 228

How Bundled Provisioning Works

In dynamic management mode, when an Polycom endpoint starts up and at designated intervals thereafter, it automatically polls for new provisioning information from the RealPresence Resource Manager system. If a bundled provisioning profile exists on the RealPresence Resource Manager system that has been associated with the endpoint, the bundled profile is sent over a secure HTTPS connection.

In this release, the RealPresence Group system, RealPresence Immersive Studio systems, and HDX system (v3.0.3 and higher) parameters that may be included in a bundled provisioned profile are limited to the following types:

- Camera configuration settings
- Monitor configuration settings
- Microphone configuration settings
- Security settings (such as password length)
- Home screen settings

Considerations for Bundled Provisioning Profiles

- You can store a maximum of 1000 bundled provisioning profiles on your RealPresence Resource Manager system.
- You cannot update software with a bundled profile.
- The software version of the endpoint must match the software version of the endpoint from which the bundled provisioning profile was made. A bundled profile is only compatible with endpoints of the same software version. If the endpoint’s software version is updated, you must create a new bundled profile.
- When using bundled provisioning profiles to provision HDX systems, you can use them with v3.0.3 or higher. Previous versions do not supported bundled provisioning profiles.
- Security and home screen settings are not included in bundled profiles for RealPresence Group systems.
- You must have the Administrator role to create bundled provisioning profiles. Users with the Device Administrator role can apply and re-assign bundled provisioning profiles.
- Be sure to give each provisioning profile a unique name.

Download a Bundled Provisioning Profile

You can download a bundled provisioning profile from any RealPresence Group system, RealPresence Immsersive Studio system, or HDX system that is registered with the RealPresence Resource Manager system. After you download a provisioning profile for a specific endpoint, all dynamically-managed HDX endpoints that you associate with this profile will receive the provisioning profile when the HDX system next polls the RealPresence Resource Manager system for new provisioning information.

For more information about bundled provisioning profiles, see How Bundled Provisioning Works on page 218.

To download a bundled provisioning profile

1 Go to **Endpoint > Dynamic Management > Bundled Provisioning Profiles**.

2 Click **Download**.

The **Download Bundled Provisioning Profile From an Endpoint** dialog lists all of the HDX systems and Group systems registered with the system.

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

4 Select the endpoint that is configured the way you want for the bundled provisioning profile.

5 Complete the **Bundled Provisioning Profile Name** and **Description** fields.

6 Click **Download**.

The system confirms that the profile downloaded successfully.

7 Click **OK**.

After downloading a bundled profile, you should associate it with selected endpoints, see Edit a Bundled Provisioning Profile on page 220.

View the List of Bundled Provisioning Profiles

Use the **Bundled Provisioning View** to see the list of bundled provisioning profiles available to dynamically managed RealPresence Group systems, RealPresence Immsersive Studip systems and HDX systems.

To view a list of bundled provisioning profiles

1 Go to **Endpoint > Dynamic Management > Bundled Provisioning Profiles**

By default the **Bundled Provisioning Profile View** displays the list of bundled provisioning profiles available for use by dynamically managed HDX systems and Group systems.

The profile list in the **Bundled Provisioning Profile View** has the following information.

Field	Description
Filter	The filter choices for bundled provisioning profiles that have been downloaded to the system. Possible values include: • **Name**—Filters by the name of the bundled provisioning profile. • **Model**—Filters by the endpoint model. • **Software Version**—Filters by the software version of the endpoint. • **Creation Date**—Filters by the date the bundled provisioning profile was downloaded and created on the system. • **Description**—Filters by the description of the bundled provisioning profile.
Name	The name assigned to the bundled provisioning profile when it was downloaded and created on the system.
Model	The exact model of endpoint to which the bundled provisioning profile applies as defined when it was downloaded and created on the system.
Software Version	Displays the software version of the endpoint from which the bundled provisioning profile was downloaded.
Creation Date	The date the bundled provisioning profile was downloaded and created on the system.
Description	The description assigned to the bundled provisioning profile when it was downloaded and created on the system.
Device Count	The number of devices that are associated with the bundled provisioning profile.

Edit a Bundled Provisioning Profile

Users with the administrator role are allowed to edit bundled provisioning profiles. When you edit a bundled provisioning profile you can rename the profile or change which devices are associated with the profile.

To edit a bundled provisioning profile

1 Go to **Endpoint > Dynamic Management > Bundled Provisioning Profiles**

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

3 Select the profile that you want to edit.

4 Click **Edit** to view the **Edit Bundled Provisioning Profile** dialog box.

5 Use the **Edit Bundled Provisioning Profile** dialog box to edit the profile and click **Ok**.

Field	Description
General Settings	
Name	Enter a name for the profile.
Description	Enter a description for the profile.
Associate Devices	

Field	Description
Filter	This list of available devices automatically lists all dynamically-managed devices of the same model and software version used for the bundled profile. The Filter allows you to filter the list of available devices. Available filters include: **Name**: Type the first few letters of the system name and press Enter. **IP Address**: Type the first numbers of the IP address of the device(s) and press Enter. **Site**: Type the first letters of the site name of which whose devices you want to view and press Enter.
Available Devices	Lists the available devices to associate with this profile. Only devices that are dynamically managed appear in the list. Use the arrows to move a device or devices to the Selected Devices list.
Selected Devices	Lists the devices that have been selected to receive this profile. Use the arrows to move a device or devices back to the Available Devices list.

Re-associate Devices with a Different Profile

Users with the administrator role can re-associate devices with a different bundled provisioning profile or no bundled profile. For example, you could use this feature if you previously associated all RealPresence Group 300 systems with a specific profile, but then downloaded an updated bundled provisioning profile that you would like to use instead.

To re-associate devices with a different bundled provisioning profile

1. Go to **Endpoint > Dynamic Management > Bundled Provisioning Profiles**
2. Select the profile from which you want to remove the associated devices.
3. Click **Re-associate Devices** to view the **Move Associated Devices** dialog box.
4. In the **Move Associated Devices** dialog box, use the **Target Bundled Profile** list to choose a profile (or None) from the to which to move the associated devices.
5. Click OK.

Delete a Bundled Provisioning Profile

When you no longer need a bundled provisioning profile, you can delete it.

1. Go to **Endpoint > Dynamic Management > Bundled Provisioning Profiles**
2. As needed, use the **Filter** to customize the list of bundled provisioning profiles.
3. Select the profile you want to delete.
4. Click **Delete**.
5. Click **Yes** to confirm the deletion.

The system confirms that the profile was deleted.

Settings included in a Bundled Provisioning Profile for an HDX

The following tables lists the settings contained in a bundled provisioning profile for an HDX system.

Field	
Home Screen Settings	
	System Name (Display) Local Date and Time (Display) System (Display) Availability Control (Display) My SIP (Display) My IP (Display) My ISDN (Display) My Extension (Display) Home Button (1-6) Speed Dial (all)
Place a call	
	Last Number Displayed Call Quality
Password Settings	
Admin Room	Minimum Length Require Lower Case Require Upper Case Require Numbers Require Special Characters Reject Previous Passwords Minimum Password Age in Days Maximum Password Age in Days Password Expiration Warning in Days Minimum Changed Characters Maximum Consecutive Repeated Characters Can contain ID or its Reverse Form

Field	
Admin Remote	Minimum Length Require Lower Case Require Upper Case Require Numbers Require Special Characters Reject Previous Passwords Minimum Password Age in Days Maximum Password Age in Days Password Expiration Warning in Days Minimum Changed Characters Maximum Consecutive Repeated Characters Can contain ID or its Reverse Form
User Room	Minimum Length Require Lower Case Require Upper Case Require Numbers Require Special Characters Reject Previous Passwords Minimum Password Age in Days Maximum Password Age in Days Password Expiration Warning in Days Minimum Changed Characters Maximum Consecutive Repeated Characters Can contain ID or its Reverse Form
User Remote	Minimum Length Require Lower Case Require Upper Case Require Numbers Require Special Characters Reject Previous Passwords Minimum Password Age in Days Maximum Password Age in Days Password Expiration Warning in Days Minimum Changed Characters Maximum Consecutive Repeated Characters Can contain ID or its Reverse Form

Field	
Meeting	Minimum Length Require Lower Case Require Upper Case Require Numbers Require Special Characters Reject Previous Passwords Minimum Password Age in Days Maximum Password Age in Days Password Expiration Warning in Days Minimum Changed Characters Maximum Consecutive Repeated Characters Can contain ID or its Reverse Form
Require Numbers: User Room	
Account Management	
	Lock Account After Failed Logins: Admin Account Lock Duration in Minutes: Admin Lock Account After Failed Logins: User Account Lock Duration in Minutes: User
Log Management	
	Percent Filled Threshold Log File Name Folder Name Transfer Frequency
Monitors	
Monitor 1	Aspect Ratio Video Format Resolution Output Upon Screen Saver Activation Display Near Video Display Far Video Display Content

Field	
Monitor 2	Aspect Ratio Video Format Resolution Output Upon Screen Saver Activation Display Near Video Display Far Video Display Content
Monitor 3	Aspect Ratio Video Format Resolution Output Upon Screen Saver Activation Display Near Video Display Far Video Display Content Display Copy of Monitor 1/2
Monitor 4	Aspect Ratio Video Format Resolution Output Upon Screen Saver Activation Loop Selected Camera to Monitor 4
People Video Adjustment	
Content Video Adjustment	
Dual Monitor Emulation	
Display Icons in a Call	
Screen Saver Wait Time	
PIP Timer	
Multipoint Setup	
	Auto Answer Multipoint Video Multipoint Mode
Cameras	
Camera 1	Name Aspect Ratio Video Quality (Motion/Sharpness setting) Source (People/Content setting)

Field	
Camera 2	Name Aspect Ratio Video Quality (Motion/Sharpness setting) Source (People/Content setting)
Camera 3	Name Aspect Ratio Video Quality (Motion/Sharpness setting) Source (People/Content setting)
Camera 4	Name Aspect Ratio Video Quality (Motion/Sharpness setting) Source (People/Content setting)
Camera 5	Name Aspect Ratio Video Quality (Motion/Sharpness setting) Source (People/Content setting)
Far Control of Near Camera	
Backlight Compensation	
Primary Camera	
Camera Pan Direction	
Quality Preference	
Dynamic People/Content Bandwidth	
Power Frequency	
Send Content When PC Connects	
Camera Icon Category	
People On Content	
	Foreground Source Background Source

Field	
Audio Settings	
Sound Effects Volume	Sound Effects Volume Incoming Video Call Tone User Alert Tone Mute Auto Answer Calls Enable Live Music Mode Mute Auto Answer Calls Enable Live Music Mode Enable Keyboard Noise Reduction Enable Polycom Microphones Enable Hawkeye Microphones
Audio Input	
	Content Input Level Line Input Level Line Input Type (Line, Mic) Line Input Cancellor Enable Enable Phantom Power (for Mic Input mode)
Audio Output	
	Line Output Mode Line Output Level VCR/DVD Output Level VCR/DVD Output On Master Audio Volume Bass Treble
Stereo Settings	
	Enable Polycom StereoSurround Stereo Auto Rotation (per Mic) Mic Mode (Left, Left+Right, Right)

Settings included in a Bundled Provisioning Profile for a RealPresence Group System and RealPresence Immersive Studio System

The following tables lists the settings contained in a bundled provisioning profile for a RealPresence Group system as well as RealPresence Immersive Studio systems.

Field	
Monitors	
Monitor 1	Enable Video Format Resolution
Monitor 2	Enable Video Format Resolution
Monitors	
Monitor 1	Enable Video Format Resolution
Monitor 2	Enable Video Format Resolution
Sleep	
Sleep	Display Time before system goes to sleep
Video Inputs	
General Camera Settings	Allow other participants in a call to control your camera Power Frequency Make this camera your main camera

Field	
Input1: Main	Model Name Display As Input Format Optimized for White Balance Brightness Color Saturation
Input2: Main	Name Display As Input Format Optimized for Backlight compensation White Balance Brightness Color Saturation
Audio	
General Audio Settings	Polycom Stereo Sound Sound Effects volume Ringtone User Alert Tones Mute Auto Answer Calls Enable Music Mode Enable Keyboard Noise Reduction Enable Polycom Microphones
Audio Input	Use 3.5 mm Input for Microphone HDMI Input (left/right) 3.5 mm (left/right)
Audio Output	Line Output Mode
Levels	Master Audio Volume Bass Treble
Security > Local Accounts	
Account Lockout	• Lock User Account After Failed Logins

Field	
Login Credentials	• Admin Room Password • User Remote Access Passowrd • Require User Login for System Access
Password Requirements	All password requirements for the following passwords: • Admin Room • User Room • Meeting • Remote Access
General Setting > Pairing > Polycom Touch Control	
Enable Polycom Touch Control	

Using Access Control Lists

The Polycom® RealPresence® Resource Manager system allows you to create Access Control Lists for dynamically-managed endpoints.

This chapter describes RealPresence Resource Manager system Access Control List operations. It includes these topics:

Understanding Access Control Lists

Users with the administrator, device administrator or area administrator role can create Access Control Lists.

An Access Control List is a whitelist of users/groups whose endpoint(s) of a particular type are allowed to authenticate with the RealPresence Resource Manager system for provisioning and video network services. Access Control Lists can only be used with endpoints that are dynamically-managed.

This is particularly useful when controlling Polycom’s soft endpoints such as CMA Desktop and RealPresence Mobile which use the provisioning credentials to authenticate with your video network.

You can use Access Control Lists to control access to the RealPresence Resource Manager system for the following endpoint types:

- Polycom HDX systems
- Polycom RealPresence Group systems
- Polycom RealPresence Immersive Studio systems
- Polycom CMA Desktop
- RealPresence Desktop
- RealPresence Mobile (multiple device models)
- Polycom VVX systems

Implementing Access Control Lists

Once you create an Access Control List for an endpoint type, all users of that endpoint type must be included on an Access Control List in order to access the RealPresence Resource Manager system for provisioning and authentication.

In other words, if you create an Access Control List and associate it with a user group, only those members of that user group can access the RealPresence Resource Manager system for provisioning and authentication.

It's important to plan your implementation of Access Control Lists. Use the following steps:

1. Determine an endpoint type of which you want to limit RealPresence Resource Manager system access.
2. Determine which user groups you want to include in the Access Control List.

If you do not create Access Control List for an endpoint type, then all users with that endpoint type are allowed to access the RealPresence Resource Manager for provisioning and authentication.

For example, if you create an **Access Control List** that includes RealPresence Mobile systems, all users of RealPresence Mobile endpoints must now be included on an **Access Control List** in order for their endpoints to be provisioned and authenticate with your video network.

However, if you have not created an Access Control List for HDX systems, all users with HDX systems managed by the RealPresence Resource Manager system can have their endpoints be dynamically managed.

Using Access Control Lists in a Multi-Tenancy Environment

You can associate an **Access Control List** with a specific area.

If you associate the Access Control List with a user group that is not in the same area as the assigned area of the Access Control List, you will be prompted to allow the RealPresence Resource Manager system to change the area of the group to match the area of the list.

If you move re-assign an Access Control List to a different area, you are prompted to allow the RealPresence Resource Manager system to change the are of the group(s) to match the area of the list.

User groups associated with an Access Area List must reside in the same area as the list.

Working with Access Control Lists

This section describes how to work with Access Control Lists and includes the following topics:

- Add a New Access Control List on page 233
- Edit an Access Control List on page 234

Add a New Access Control List

You can create an Access Control List that includes all endpoints of a particular device type(s) within a user group. For example, you can create an Access Control List that enables all RealPresence Group systems that belong to a user group to be dynamically provisioned.

To add a new Access Control List

1 Go to **Endpoint > Dynamic Management > Access Control Lists**.

The **Access Control Lists** page appears.

2 Click **Add**.

3 In the **Add Access Control List** dialog box, complete the following fields in the General Info tab.

Access Control List Name	Enter a unique name for the Access Control List.
Description	Enter a description for the Access Control List.
Assign Area	If areas are enabled, and you have permission to manage more than one area, use the **Assign Area** drop-down list to assign the Access Control List to an area. The drop-down list does not appear if areas are not enabled or the user does not have permission to assign an area.

4 Click **Associate Device Types**.

5 In the **Associated Device Types** section, select and move the desired **Available Device Types** endpoint types(s) to **Selected Device Types** list.

6 When you include a RealPresence Mobile endpoint, you need to also choose the device model to include in the Access Control List.

- In the **Select the RealPresence Mobile device model** section, select and move the desired device models to the **Selected Device Model** list.

  All device models are included by default.

7 Click **Associated Groups.**

8 Use the **Search Group** field to find the group(s) you want to associate with this Access Control List.

9 In the **Search Results** section, select and move the desired group(s) to **Selected Groups** list.

10 Click **Ok**.

Edit an Access Control List

You can edit an Access Control List at any time. You can add or delete IP addresses or the groups associated with the list. When you make changes to an access control list, the changes take place immediately.

To edit an Access Control List

1 Go to **Endpoint > Dynamic Management >Access Control Lists**.

The **Access Control Lists** page appears.

2 Select an access control list.

3 Click **Edit**.

4 Modify any of the fields and click **Ok**.

> If you change the area of the access control list, you are asked to confirm that all groups associated with the list will also be changed to the new area.

Delete an Access Control List

You can delete an access control list. Deleting an access control list may deny user groups associated with the list access to RealPresence Resource Manager conferencing services. Remember to re-assign any user groups to a new access control list if you need them to continue to be able to authenticate.

To delete an access control list

1 Go to **Endpoint > Dynamic Management >Access Control Lists**.

The **Access Control Lists** page appears.

2 Select an access control list.

3 Click **Delete**.

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

Dynamic Provisioning of Endpoints for SIP Server Integration

The Polycom® RealPresence® Resource Manager system allows you to dynamically provision some Polycom endpoints with the SIP server integration information by them with the SIP credentials and SIP settings they need.

SIP settings can only be provisioned when you use dynamic management. You can provision SIP by using both a Network provisioning profile and an Admin Config provisioning profile. You cannot use scheduled or bundled provisioning to provision SIP settings.

For more information about Network provisioning profiles , see Network Provisioning Profiles on page 185.

You can configure the RealPresence Resource Manager system to dynamically provision SIP settings for the following SIP servers:

- Standard (a SIP server that meets SIP standards)
- Microsoft Lync
- BroadSoft BroadWorks
- Polycom DMA system
- Siemens OpenScape
- Avaya Aura Session Manager
- Cisco Unified Communications Manager

This section includes the following topics:

- SIP Provisioning Considerations on page 235
- Provision Endpoints with SIP Server Settings on page 236

SIP Provisioning Considerations

- SIP settings are configured using network provisioning profiiles.
- If the SIP server uses a different authentication directory than your RealPresence Resource Manager system and requires unique authentication for each endpoint, you need to ensure that users have existing SIP URIs before provisioning SIP settings.
- Provisioning Microsoft SIP requires additional steps, see Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration on page 240.

SIP Server Authentication Requirements

You must understand your SIP server’s authentication requirements when you provision SIP settings for endpoints managed by the RealPresence Resource Manager system.

SIP server authentication requirements differ according to your environment.

- If your SIP server does not require credentials, you do not need to indicate any credentials to use when provisioning.
- If your SIP server requires a common username and password for all endpoints registering to the SIP server, you need to explicitly provision that username and password to applicable endpoints.
- If your SIP server uses the same authentication database (i.e., Microsoft Active Directory) as the RealPresence Resource Manager system, you need to use the RealPresence Resource Manager system provisioning credentials.
- If your SIP server does NOT use the same authentication database as the RealPresence Resource Manager system and requires unique usernames and passwords for each endpoint, you need ensure that each user has an existing SIP URI before you can use Network provisioning profiles to provision SIP settings.

Provision Endpoints with SIP Server Settings

The RealPresence Resource Manager system supports the integration with various SIP servers by provisioning endpoints SIP settings they need.

After you provision endpoints with SIP settings, all endpoints receive directory information from one of those servers. You are no longer using the enterprise directory or the other directory functions in the RealPresence Resource Manager system.

The RealPresence Resource Manager system supports SIP to establish conference connections. If you want to use SIP, you must enable it and configure SIP settings. You must also ensure that users have SIP URIs.

To provision endpoints with the information required to integrate with these SIP servers, you must complete the following tasks:

- Creating Authentication Information for SIP Endpoints on page 236
- Import SIP URI Data on page 237
- Provision SIP Settings for SIP Server Integration on page 238

Creating Authentication Information for SIP Endpoints

To have the RealPresence Resource Manager system dynamically provision a Polycom endpoint for SIP integration, the endpoint must use the same credentials (username and password) to access both the SIP server and the RealPresence Resource Manager system. Only then can the RealPresence Resource Manager system provision SIP settings.

If the SIP server uses a third-party database for authentication that the RealPresence Resource Manager system is not aware of, you need to import both the user information and SIP URI information from the SIP server.

1. Create a RealPresence Resource Manager system local user account for the endpoint that matches the username and password. To save time, you can import the users that you need, see Import Local Users on page 295.
2. Import SIP URI data for those users, see Import SIP URI Data on page 237.

> **Note**
>
> The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

Import SIP URI Data

After you enable and configure SIP, you must import your endpoint SIP URI information from your SIP server. The SIP URI is used as the endpoint's address.

> If you are using Microsoft as your SIP server, you do not need to import SIP URI data. The RealPresence Resource Manager system can retrieve the SIP URI from the enterprise directory.

1. Create a CSV file in the format described here. The import requires a CSV file in the following format:

```
domain,username,deviceType,SIPURI,devicename
```

where:

- `domain`—Specifies the domain the user uses to log in to the RealPresence Resource Manager system.
- `username`—Specifies the RealPresence RealPresenceResource Manager system user name.
- `deviceType`—Specifies the device type (valid values are HDX, VVX, CMADesktop, RPMobile, RPDesktop, GroupSeries or All_Types).
- `SIP URI`—Specifies the SIP URI for this user.

For example, this import reserves the SIP URI `johndoe@example.com` for all device types for the John Doe user:

```
local,johndoe,All_Types,johndoe@example.com
```

> When working on a double-byte system such as Chinese or Japanese, you need to ensure the .CSV file is encoded using UTF-8. CSV files created with Microsoft Excel do not support UTF-8 encoding. When exporting as CSV, you need to save the file first and then open it in an application that supports UTF-8 encoding. When importing, you need to be sure that the file has been saved with UTF-8 encoding. Polycom recommends using a tool such as NotePad ++ to save the CSV file using UTF-8 encoding.

2 From the RealPresence Resource Manager system, go to **User > Users**.

   a Click **Import User Aliases**.

   b Navigate to the CSV file, select it, and click **Open**.

   Whenever you add new users or rooms or need change a SIP URI, you must provide SIP URI data. For the methods available for editing the SIP URI, see Edit SIP URI Data on page 238.

Edit SIP URI Data

You can edit SIP URI data in the following ways:

- Upload a CSV file that has changes or new data. Data in the CSV file is added to any existing data. For information about the CSV file format and the upload process, see Import SIP URI Data on page 237. You must be using Internet Explorer or Google Chrome to upload a file.
- Edit individual users or rooms. For each RealPresence Resource Manager system user or room, you can add or edit the SIP URI in the **Dial String Reservations** section of the **Edit User** or **Edit Room** dialog box.

Provision SIP Settings for SIP Server Integration

SIP settings are dynamically provisioned with a network provisioning profile. This procedure describes how to change existing network provisioning settings so that they provision integration with a SIP server.

Be sure to enable SIP and configure the servers, protocol, and credentials needed for your SIP sever.

To provision SIP for integration with a SIP server

1 Go to **Endpoint > Dynamic Managment > Provisioning Profiles**.

2 Select the **Network Provisioning Profile** you want to edit and click **Edit.**

3 In the **Edit Profile** dialog box, click **SIP Settings** and select these options.

Fields	Description
Enable SIP	Specify whether to enable SIP calls.
Automatically Discover SIP Servers	The RealPresence Resource Manager system will issue a DNS query to locate the SIP server and provision that information to endpoints.
Proxy Server	Specify the IP address or DNS name of the SIP proxy server for the network.
Backup Proxy Server	Specify the IP address or DNS name of a backup proxy server for the network.
Registrar Server	Specify the IP address or DNS name of the SIP registrar server for the network. • In an Microsoft Office Communications Server 2007 or Microsoft Lync Server 2010 environment, specify the IP address or DNS name of the Office Communications Server or Lync Server server. • If registering a remote HDX system with an Office Communications Server Edge Server or Lync Server Edge Server, use the fully qualified domain name of the access edge server role.

Fields	Description
Backup Registrar Server	Specify the IP address or DNS name of a backup SIP registrar server for the network.
Transport Protocol	Indicates the protocol the 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. • TCP provides reliable transport via TCP for SIP signaling. • UDP provides best-effort transport via UDP for SIP signaling. • TLS provides secure communication of the SIP signaling. TLS is available only when the system is registered with a SIP server that supports TLS. When you choose this setting, the system ignores TCP/UDP port 5060.
Server Type	Specify the SIP server type. • Standard: • Polycom: • Avaya: • BroadSoft: • Cisco: • Microsoft: If you are integrating with a Microsoft Server, you must also provision a group for the endpoint, see Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration on page 240. • Siemens:
Verify Certificate	Enable this option when the endpoint system’s certificate should be verified by the certificate authority.
Use Endpoint Provisioning Credentials	Enable this option when the endpoint system should use the credentials the user entered at the endpoint to use for authenticate when registering with a SIP registrar server.
Common SIP User Name	Specify the name to use for authentication when registering with a SIP registrar server, for example, `msmith@company.com`. If the SIP proxy requires authentication, this field and the password cannot be blank.
Use Enterprise URI	Enable this option with the endpoint should use the SIP URI of the enterprise user (domain user).
Common SIP Password	Specify the password that authenticates the system to the registrar server.

4 Click OK.

5 You need to ensure that you have created a provisioning rule that applies this network provisioning profile to the intended site and endpoints.

Provision Group for Microsoft Lync or Microsoft Office Communications Server Integration

You must set up the Microsoft Lync or Office Communications Server group that needs to be provisioned to endpoints in each Admin Config provisioning profile. This controls the directory that endpoints can see.

- You cannot provision integration with a Microsoft Lync or Office Communications Server via scheduled provisioning.
- If the endpoint being provisioned is not capable of integration with a Microsoft Lync or Office Communications Server, the endpoint will ignore this settings.
- The group setting here applies to both Microsoft Lync and Office Communication Server.

To provision integration with Microsoft Lync or Office Communications Server

1. Go to **Endpoint > Dynamic Management > Provisioning Profiles**.
2. In the **Provisioning Profiles** page, select the **Admin Config** profile of interest and click Edit.
3. In the **Provisioning Fields** dialog box, click **Microsoft Lync Settings** and enter a **Group Name**.

   The Group Name is the group set in the Microsoft Lync Server or Office Communication Server.
4. Click **OK**.

Microsoft Directory Considerations

When Polycom endpoints are registered with a Microsoft Lync Server or Office Communications Sever, the SIP server replaces the RealPresence Resource Manager system as the presence and directory service provider. However, the system continues to act as manager for these endpoint systems.

If you want your directories to include endpoints such as CMA Desktop that are not registered to the Microsoft SIP server, you need to select Standard as your SIP server when provisioning settings.

You still need to use the RealPresence Resource Manager system provisioning credentials when provisioning the SIP settings to the endpoint.

Dynamically Managing a RealPresence Access Director System

The Polycom® RealPresence® Resource Manager system allows you to use RPAD server provisioning profile as a way to dynamically manage a RealPresence Access Director system.

You can use an RPAD server provisioning profile to dynamically manage the RealPresence Access Director system and configure it with the right network information to allow for firewall traversal in your video infrastructure environment.

This chapter describes RealPresence Resource Manager system RealPresence Access Director system provisioning operations. It includes these topics:

Dynamically Managing a Polycom RealPresence Access Director System

Perform the following steps to dynamically add and provision a RealPresence Access Director system:

1. Create a Site for the RealPresence Access Director System on page 241
2. Create a RPAD Server Provisioning Profile on page 242
3. Create a Network Provisioning Profile for Endpoints on page 242
4. Create a Provisioning Rule and Associate it with All Related Profiles on page 243
5. Create a User Account for the RealPresence Access Director System on page 243

Create a Site for the RealPresence Access Director System

You should create a site that includes the subnet on which the RealPresence Access Director resides. You'll need to add the RealPresence Access Director system's internal IP to the subnet of the site.

See Add a Site on page 379 for more information about adding a site.

> You cannot use the same site for more than one RealPresence Access Director system. You must create a unique site for each RealPresence Access Directory system that you use.

Create a RPAD Server Provisioning Profile

You can dynamically provision a RealPresence Access Director system with the a RPAD server provisioning profile.

An RPAD server provisioning profile includes all applicable settings for a RealPresence Access Director system.

The RealPresence Access Director system should be configured with the IP addresses of the Polycom DMA system as the gatekeeper and SIP server within your environment.

With RPAD server provisioning profiles, you can ensure that a RealPresence Access Director system has the optimal and correct firewall traversal settings to support endpoints that will depend on it for firewall traversal.

As soon as an RealPresence Access Directory system configured to use the RealPresence Resource Manager for its provisioning server, it starts polling for provisioning profile updates. So to ensure out-of-box usability, the RealPresence Resource Manager system comes with a default RPAD Server Provisioning Profile.

The default RPAD server provisioning profile cannot be associated with any provisioning rules.

You need to add a new RPAD server provisioning profile in order to customize the settings of your RealPresence Access Director system.

To create a RPAD provisioning profile

1. Go to **Endpoint > Dynamic Management > RPAD Provisioning Profiles**.
2. Click **Add**.
3. In the **General Info** section of the **Add New Profile** section,
   - ➢ Enter a name for the new RPAD server provisioning profile.
   - ➢ Select **Server Provisioning Profile** from the drop-down list.
4. As needed, edit the server provisioning details and click **Apply**. For information about these details, see Available Settings for a RPAD Server Provisioning Profile on page 243.
5. Click **OK**.

Create a Network Provisioning Profile for Endpoints

You need to create a network provisioning profile to apply to all dynamically managed endpoints within the same site as a RealPresence Access Director system. These endpoints need to be provisioned to use the RealPresence Access Director system external IP address for all of their network settings.

Ensure that all of the network settings (gatekeeper, presence server, SIP server, and directory) are set to the external IP address of the RealPresence Access Director system.

For example, instead of the IP address of the DMA system’s gatekeeper, you should provision endpoints to use the external IP address of the RealPresence Access Director system as the gatekeeper IP.

For more information about creating a network provisioning profile, see Network Provisioning Profiles on page 185.

Optionally, create an Admin Config Provisioning Profile

If you want to provision the endpoints that use the RealPresence Access Director system with specific admin configuration settings, you can create an **Admin Config** profile to use.

For information about creating Admin Config provisioning profiles, see Admin Config Provisioning Profiles on page 194.

Create a Provisioning Rule and Associate it with All Related Profiles

You need to create a provisioning rule that includes a condition that defines that the rule be applied to the site that includes the RealPresence Access Director system.

For example,

```
(Site.Site = RealPresence Access Director Site)
```

At a minimum, the provisioning rule must contain this site condition.

Associate both the **RPAD Server Provisioning** profile and the **Network Provisioning** profile (for endpoints) with the rule. You can also include an **Admin Config** profile if needed. This ensures that all endpoints within the subnet of the site created for the RealPresence Access Director are provisioned with the correct settings. It also provisions the RealPresence Access Director system.

For detailed instructions on how to create a provisioning rule, see Creating Dynamic Provisioning Rules on page 199.

Create a User Account for the RealPresence Access Director System

You need to create a user account for RealPresence Access Director system to use to authenticate with the RealPresence Resource Manager system's provisioning service.

For more information about creating user accounts, see Manage Users on page 289.

Use this account to register the RealPresence Access Director system with the RealPresence Resource Manager system's provisioning service.

See the *Polycom RealPresence Access Director System Administrator's Guide* for more information about provisioning the RealPresence Access Director

Available Settings for a RPAD Server Provisioning Profile

Field	For the RealPresence Access Director system being provisioned...
RPAD Settings	
Time Server	Specify the time display format.

Field	For the RealPresence Access Director system being provisioned...
Primary Time Server	Specify whether to connect to a time server for automatic system time settings. Currently, the RealPresence Access Director system can only be provisioned with a **Manual** setting. If you use the **Auto** setting, the RealPresence Access Director system will behave as if the Time Server is set to **Off**. Select **Auto** to require that the RealPresence Access Director system synchronize with an external time server that is identified by a network domain controller. Because it is identified by a network domain controller, you do not need to enter the IP address of the time server. Select **Manual** to require that the RealPresence Access Director system synchronize with an external time server that may not be identified by a network domain controller. In this case, you must also enter the IP address of the time server in the **Time Server Address** field. If **Time Server** is set to **Off**, or if the **Time Server** is set to **Manual** or **Auto** but the endpoint system cannot connect to the time server, the date and time must be manually reset at the endpoint.
Primary Time Server Address	Specify the address of the primary time server when **Time Server** is set to **Manual**.
Secondary Time Server Address	Specify the address of the secondary time server when **Time Server** is set to **Manual**.
Provisioning Polling Interval	Specify the frequency at which the RealPresence Access Director system polls the RealPresence Resource Manager system for new provisioning information. By default, this interval is 60 minutes. For performance reasons, the minimum positive value for this interval is 5 minutes. There is no maximum value enforced.
Heartbeat Posting Interval	Specify the frequency at which the RealPresence Access Director systems poll the Resource Manager system for a heartbeat.
Server Status Posting Interval	
RPAD Settings 2	
Enable IP H.323	Specify whether to enable IP H.323 calls.
Gatekeeper IP Address	When **Use Gatekeeper** is set to **Specify**, enter the gatekeeper IP address in this field.
Enable SIP	Specify whether to enable SIP calls and enable the provisioning of SIP settings.
Proxy Server	Specify the IP address or DNS name of the SIP proxy server for the network. If you leave this field blank, the registrar server is used. Enter the Polycom DMA signalling IP address in this field.
Registrar Server	Specify the IP address or DNS name of the SIP registrar server for the network. Enter the Polycom DMA signalling IP address in this field.
Use Default Directory Server	When this field is marked, the RealPresence Resource Manager system serves as the default directory server for the RealPresence Access Director system.

Field	For the RealPresence Access Director system being provisioned...
Directory Server	
Verify Certificate	Enable this option when the RealPresence Access Director system's certificate should be verified by the certificate authority.
Use Default Presence Directory Server	
Presence Server	Use the **Presence Server** field enter the IP address of the presence server you wish to use.
Verify Certificate	Enable this option when the RealPresence Access Director system's certificate should be verified by the certificate authority.

Network Device Management

This section provides an introduction to the Polycom® RealPresence® Resource Manager network device management functionality and operations. It includes:

Understanding Network Device Management

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system's network device management functions. This chapter includes these topics:

- Overview of Network Devices
- Monitoring Network Devices

Network devices include any non-endpoint device that the RealPresence Resource Manager system manages or is aware of.

You must have the Device Administrator role to add new network devices to the system or edit their properties. If your system supports multi-tenancy and areas have been enabled, users with the Area Administrator role can also perform some device management tasks.

The remaining user roles can view network devices, but not add new ones or modify settings.

Overview of Network Devices

The RealPresence Resource Manager system supports these network device types:

- MCUs — See Managing MCU Bridges on page 251
- Polycom DMA™ system — See Managing a DMA System on page 263
- DMA Pool Orders — Managing DMA Pool Orders on page 268
- Polycom VBPs — See Managing Border Controllers and Firewalls on page 271
- SBCs (session border controls)— See Managing Border Controllers and Firewalls on page 271
- Polycom RealPresence Access Director systems— See Managing Border Controllers and Firewalls on page 271.

Monitoring Network Devices

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

- **Monitor View**—Displays the list of all manageable and registered network devices. Use this view to manage network devices.
- **VBPs** (Video Border Proxy systems)—Displays the list of Polycom VBP systems registered to the Resource Manager system. Use this view to add, edit, or delete VBP systems.

- **SBCs** (Session Border Control systems)—Displays the list of SBC systems registered to the Resource Manager system. Use this view to add, edit, or delete SBC systems.
- **MCUs** (Microprocessing Control Units)—Displays the list of Polycom MCUs (Polycom RMX systems) registered to the Resource Manager system. Use this view to add, edit, or delete MCUs.
- **DMA**—Displays the Polycom DMA system registered to the Resource Manager system. Use this view to add, edit, or delete a DMA system.
- **DMA Pool Orders**—Displays the list of Polycom DMA Pool Orders associated with the DMA system that is registered to the Resource Manager system. Use this view to view and edit DMA pool orders.
- **RPADs**—Displays the list of RealPresence Access Director systems registered to the Resource Manager system. Use this view to add, edit, or delete RealPresence Access director systems.

The **Network Device > Monitor View** has the following information:

Section	Description
Views	The views you can access from the page.
Actions	The set of available commands. The constant command in the **Network Device** views is **Refresh**, which updates the display with current information.
Network Device List	The context-sensitive **Network Device** list for the selected view.
Device Summary	Information about the network device selected in the network device list.

Monitor View

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

Considerations for Multi-Tenancy

Users with area roles will see only those network devices assigned to the area they manage.

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

Field	Description
Filter	Use the filter choices to display other views of the **Network Device** list, which include: • **Type** - Filters the list by device type. • **Alerts** - Filters the list by alert type: Help, Error, or Warning • **Connection Status**- Filters the list by connection status: In a Call, Online, or Offline • **Name** - Filters the list by system name entered • **IP Address** - Filters the list by IP address entered • **Alias** - Filters the list by the alias entered • **Site** - Filters the list by site location entered • **Area not same as Site's Area** - Available only when Areas are enabled. This allows you to filter on devices that may have been added to a different area than their site's area. A device and the site it belongs to must be assigned to the same area. This filter allows you to troubleshoot any misplaced devices. • **Area** - Available only when Areas are enabled. Filters the list by the area with which the device is associated. You can only view area-specific information for area(s) that you have permission to manage.
Status	The state of the network device. Possible values include: • Online ✓ • Offline ⊘ • In a call ⇔ • Unknown ? • Device alert ! • Gatekeeper not applicable
Name	The system name of the network device.
Type	The type of network device.
IP Address	The IP address assigned to the network device.
Site	The site to which the network device belongs. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Area	Available only when Areas are enabled. The area with which the network device is associated. Users can only view area information for the areas they have been assigned to manage.

Actions in the Monitor View

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

Action	Use this action to...
Available for all device types	
Add	Manually add a network device to the RealPrescne Resource Manager system or find a network device on the network. You can search for devices using DNS or IP address.
Edit	Change connection settings for the selected network device. Note that if this is a managed device, the device may overwrite settings entered manually.
Delete	Delete the selected network devices.
View Details	Display all of the **Device Details** for the selected network device.
Available for only selected network device types	
Manage	Open the selected network device's management interface in a separate browser window.
Associate Area	Available only for DMA Pool Orders and when **Areas** are enabled. Associate the selected DMA Pool Order to an area so that only specified area users can use it to schedule conferences. Users can only view area information for the areas they have been assigned to manage. Only DMA Pool Orders can be associated with an area via this menu. You can associate an RMX system with an area using the Edit option. Other network devices cannot be associated with an area.

Managing MCU Bridges

This chapter describes how to perform the Polycom® RealPresence® Resource Manager system MCU bridge management tasks. It includes these topics:

MCU View

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

The **MCU** View allows you to view more detailed information about the MCUs that your system manages.

View Device Details

To view detailed information about a managed MCU bridge

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

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

Add an MCU Manually

This topic describes how to add an MCU to a RealPresence Resource Manager system.

Polycom RMX systems cannot be managed by two management sytems at the same time. When your deployment includes a Polycom DMA system, you can manage an RMX system either in the DMA system or with the RealPresence Resource Manager, not both.

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

When you add an MCU device, MCU network services are added automatically at the time the IP card registers with the RealPresence Resource Manager system.

> - Polycom MGC systems may only have H.323/H.320 services.
> - Once an MCU registers with the RealPresence Resource Manager system, if you change an MCU service on the MCU, the update does not automatically get sent to the RealPresence Resource Manager system. To update the system, you must refresh the device, see Edit an MCU Bridge on page 253.

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

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

To add an MCU bridge or find an MCU on the network

1. Go to **Network Device > MCUs** and click **Add**.
2. In the **Add New Device** dialog box, select the **Device Type** of interest.
3. Enter either the **IP Address** or the **DNS Name** of the MCU.
4. Enter the **Admin ID** and **Password** for the MCU.
5. Click **Find Device**.
   - ➢ If the RealPresence Resource Manager system can find the MCU on the network, the **Add New Device** dialog box is populated with information retrieved from the MCU. Review any information retrieved from the MCU.
   - ➢ If the RealPresence Resource Manager system cannot find the MCU on the network, a **Device Not Found** dialog box appears.
6. Click **OK**.

7 Complete the **Identification**, **Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading** sections of the **Add New Device** dialog box.

For more information, see View Device Details on page 251.

At a minimum, assign the MCU a **System Name.**

> **When Integrating with a DMA System**
>
> - If your system integrates with a Polycom DMA system, make sure your MCU system name includes a qualifier that indicates to the DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, ***ResourceManager_RMX10***.
> - An RMX system can be managed by the RealPresence Resource Manager or the Polycom DMA system, not both.

Pay particular attention to the **Capabilities** options, because these settings determine how the MCU is used throughout the RealPresence Resource Manager system.

8 Click **Add**.

The MCU appears in the **Network Device** list. By default, the system:

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

Edit an MCU Bridge

To edit an MCU from the RealPresence Resource Manager system

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

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

3 Select an MCU and click **Edit.**

4 Complete the **Identification**, **Addresses, Capabilities, MCU Services, MCU Resources, and MCU Cascading** sections of the **Edit Device** dialog box.

At a minimum, assign the MCU a **System Name**.

Field	Description
Identification	
Device Type	The type of MCU.
IP Address	The assigned IP address of the MCU

Field	Description
DNS Name	The DNS name of the MCU.
System Name	The name of the MCU. • MCU names must be unique. • The name must be in ASCII only and may have an unlimited number of characters. Spaces, dashes, and underscores are valid. • When retrieved from the MCU, the name is taken from the H.323 ID if the MCU registered with the gatekeeper and it is a third-party system. In other cases, it is the system name, which might be different than the H.323 ID.
Description	A free-form text field (Extended ASCII only) in which information about the MCU can be added
Site	The network site for the MCU. By default, MCUs are added to the **Primary Site**.
Serial Number	The serial number (ASCII only) of the MCU.The serial number displays if the MCU is registered successfully or is managed.
Software Version	The version of the software installed on the MCU (ASCII only). The MCU provides the version number if it registered successfully or is managed.
HTTP URL	(Polycom RMX systems only) The management URL for the endpoint, if available (ASCII only). This URL allows the RealPresence Resource Manager system to start the endpoint ‘s management system using the **Manage** function. All Polycom endpoints allow device management through a browser. For these endpoints, this field is completed when the endpoint registers with the Resource Manager system. For third-party endpoints that do not register using an IP address, you must enter the URL.
HTTP Port	(Polycom RMX systems only) The HTTP port number for the MCU communications. The MCU provides the port number if it registered successfully and is managed. By default, in non-secure (HTTP) mode, the RealPresence Collaboration Server uses port 80 and in secure (HTTPS) mode, the RealPresence Collaboration Server uses port 443.
Area	The area in which the MCU resides. This field is only visible when Areas are enabled and the user manages more than one area. A user can only view area-specific information for an area(s) that he has permission to manage.
Addresses	
DNS Name	The DNS name for the MCU.
ISDN Video Number	The country code + city/area code + phone number for the MCU.

Field	Description
Capabilities	
Supported Protocols	The communications protocols that the MCU can support. Possible values include: • **IP (H.323)** - A standard that defines the protocols used for multimedia communications on packet-based networks, such as IP. • **ISDN (H.320)** - A standard that defines the protocols used for multimedia communications on switched networks, such as ISDN. • **IP (SIP)** - A standard that defines the protocols used for multimedia communications on SIP networks. The MCU automatically provides the protocols if it registered successfully or is managed. Polycom MGC systems may only have H.323/H.320 services.
Capabilities Enlabled	Capabilities to enable on this MCU. Options are: • **MCU** - The device can act as a control unit for multipoint conferences. • **Available to Schedule** - Select this option to make the MCU available to users who are scheduling conferences.
MCU (Network) Services	
Service Type	The available network services may include: • **H.323 Service**—Indicates a connection to an IP network using the H.323 protocol. • **SIP**—Indicates a connection to an IP network using the SIP protocol. • **H.323 & SIP Service**—Indicates a connection to an IP network using both H.323 and/or SIP protocols • **H.320 Service**—Indicates a connection to an ISDN phone line using the H.320 protocol.
Service Name	A descriptive name for the network service.
Priority	The priority set for the network service as compared to other services when it was created.
MCU Resources	
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	(Not available for MGC systems) Maximum number of video ports available on the MCU. See View Bridge Ports on page 257
Max Transcoding Ports	(MGC MCUs only) Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.

Field	Description
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Numeric ID	The IP number that conference participants dial to access the IVR prompt to join a conference.
Entry Queue ISDN Number	The ISDN number that conference participatns dial to access the IVR prompt to join a conference.
Max CP Resolution	Set this to the highest available video format. Choices are: HD1080, CIF, SD15, SD30, and HD720. Refer to the *RMX 2000/4000 Administrator's Guide* for more information about this field. Not available for MGC systems.
Max Bandwidth Capacity (Kbps)	The maximum bandwidth supported by the Polycom RMX MCU. Not available for MGC systems.

5 Optionally, you can refresh the MCU to use the settings from the MCU itself. To do this, click **Refresh Device**.

6 Click **Update**.

Delete an MCU Bridge

When you delete an MCU from the system, it is no longer managed and cannot be used on conferences.

To delete an MCU from the RealPresence Resource Manager system

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

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

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

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

The **MCU** list is updated.

View Bridge Hardware

To view the hardware configuration of a bridge

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

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

3 In the MCU list, select the bridge of interest and click V**iew Hardware**.

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

View Bridge Services

To view the network services available on the bridge

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

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

View Bridge Conferences

To view information about the conferences resident on the bridge

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

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

   The **Area** and **Billing Code** fields are only visible when Areas are enabled and the user manages more than one area.

   A user can only view area-specific information for an area(s) that he has permission to manage.

View Bridge Ports

The RealPresence Resource Manager system reports port numbers based on resource usage for CIF calls. Version 8.1 and later Polycom MCUs report port numbers based on resource usage for HD720p30 calls. In general, 3 CIF = 1 HD720p30, but it varies depending on bridge/card type and other factors.

See your Polycom RealPresence Collaboration Server or RMX system documentation for more detailed information about resource usage.

This option is not available for Polycom MGC systems.

To view information about the bridge ports

1. Go to **Network Device > MCUs.**
2. As needed, use the **Filter** to customize the MCU list.
3. In the MCU list, select a bridge and click **View Ports**.

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

View Bridge Meeting Rooms

To view information about meeting rooms on a bridge

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

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

View Bridge Entry Queues

To view information about entry queues on a bridge

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

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

View Bridge Gateway Conferences

To view information about gateway conferences on a bridge

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

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

MCU Device Details

This chapter identifies the fields found in the MCU Device Detail section of the Polycom® RealPresence® Resource Manager system interface. It includes:

- MCU H.320 Services on page 259
- MCU H.323 & SIP Services on page 260
- MCU Resources—Polycom RMX Platform on page 260
- MCU Resources—Polycom MGC Platform on page 261
- MCU Device Summary Information on page 261

Users with the Device Administrator role or Area Administrator role can view MCU device details.

MCU H.320 Services

Field	Description
MCU H.32O Service	
Service Name	Name of the H.320 ISDN service
Channels	Number of 64K channels dedicated to the MCU
Number Range	Dial-in number range of service. These ISDN numbers are available on an MCU for all endpoints to use. Also called direct inward dialing (DID).
Local Prefix	The prefix required to place a call to a local number outside the enterprise. For example, if you dial 9 to reach an outside line, the **Local Prefix** is 9.
Non-Local Prefix	The prefix required to dial long distance. For example, in certain states in the United States, you must dial 1 before you can dial a non-local number.
International Prefix	The prefix required to dial an international number. For example, in many countries, the international prefix is 00.
Local Area Code	A list of local area codes, separated by commas
Priority	The priority order for this service

MCU H.323 & SIP Services

Field	Description
Service Name	The name of the H.323 service (ASCII only) defined in the MCU.
Dialing Prefix	Prefix to select this service. The prefix for the MGC is located in the H.323 Service Properties dialog box of the MGC Manager.
Service IP Address	IP address associated with this network service and with this H.323 card in the MCU.
Alias	Alias for the service defined in the MCU. **Note** Polycom recommends using E.164 as the alias for this service. The number that is dialed if the endpoints are registered with the same gatekeeper. If the endpoints are not registered with the same gatekeeper, they use their assigned IP address to connect.
Port	Number of IP connections available.
Priority	The priority order for this service.

MCU Resources—Polycom RMX Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Video Ports	Maximum number of video ports on which participants can be connected.
Max Total Participants	Maximum number of total video participants allowed at once on this MCU.
Use Entry Queue	Indicates whether the RMX device supports an IVR.
Entry Queue Number ID	The number that conference participants dial to access the IVR prompt to join a conference.
Entry Queue ISDN Number	The number that conference participants dial to access the IVR prompt to join a conference.

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

Field	Description
Max Voice Ports	Set this to the maximum number of audio ports configured on the RMX device. Refer to the *RMX 2000/4000 Administrator’s Guide* for more information about this field. **Note** Up to 10 blocks of RMX video ports can be converted to 50 audio-only ports, up to a maximum of 200 audio-only ports.
Max CP Resolution	Set this to the highest available video format. Choices are: HD1080, CIF, SD15, SD30, and HD720. Refer to the *RMX 2000/4000 Administrator’s Guide* for more information about this field.
Max Bandwidth Capacity (Kbps)	The maximum bandwidth to the Polycom RMX system.

MCU Resources—Polycom MGC Platform

Field	Description
Max Total Conferences	Maximum number of total conferences allowed at once on this MCU.
Max CP Conferences	Maximum number of continuous presence (CP) conferences allowed, based on the number of licenses available.
Max Total Participants	Maximum number of total MCU participants allowed at once on this MCU.
Max Transcoding Ports	Maximum number of transcoding ports on which both ISDN and IP participants can be connected.
Use Entry Queue	Indicates whether the MGC device supports an IVR.
Entry Queue Number ID	The IP number that conference participants dial to access the IVR prompt to join a conference.
Entry Queue ISDN Number	The ISDN-allocated phone number of the IVR. ISDN devices only.

MCU Device Summary Information

The **Device Summary** information for MCUs in the **Monitor View** section includes the following fields.

Field	Description
Name	The name of the device.
Type	The type of device.
ID	The system-generated ID for the device.

Field	Description
IP Address	The assigned IP address of the device.
Area	Area with which the device is associated. This field is only available when Areas are enabled and the RealPresence Resource Manager user is given a role that allows them to view area information.
Site	The network site for the device. By default, devices are added to the **Primary Site**. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
ISDN Video Number	For ISDN devices only, the country code + city/area code + phone number for the device. When you add an endpoint without native ISDN, the ISDN gateway, country code, and area code are not captured. The Resource Manager system only supports native ISDN.
Software Version	The version of the software installed on the device (ASCII only). The device provides the version number if it registered successfully or is managed.
Serial Number	The serial number (ASCII only) of the device.The device provides the serial number if it registered successfully or is managed.
Available to Schedule	Select this option to make the device available when users are scheduling conferences. **Note** The **Available to schedule** field is disabled for RMX and MGC devices.
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. • **SIP** - A standard that defines the protocols used for multimedia communications on SIP networks. The device automatically provides the protocols if it registered successfully or is managed.
Capabilities Enabled	Capabilities to enable on this device. Options are: • **MCU** - The device can act as a control unit for multipoint conferences • Available to Schedule The MCU provides the capability if it registered successfully or is managed. **Note** Currently, RMX MCUs cannot be Gateway devices.

Managing a DMA System

This chapter describes how to perform the Polycom® RealPresence® Resource Manager system network device management tasks. It includes:

- Using a Polycom DMA System with RealPresence Resource Manager System
- Working with a Polycom DMA System
- Managing DMA Pool Orders

Using a Polycom DMA System with RealPresence Resource Manager System

You can integrate your RealPresence Resource Manager system with a Polycom DMA system to take advantage of the DMA system's two main functions: Conference Manager function and the Call Server (gatekeeper and SIP proxy/registrar) function, described below.

- Conference Manager
  - ➢ Provides a highly reliable and scalable multipoint conferencing solution that distributes voice and video calls across multiple media servers (MCUs), creating a single seamless resource pool. The system essentially behaves like a single large MCU, which greatly simplifies video conferencing resource management and improves efficiency.
  - ➢ Supports up to 64 MCUs. MCUs can be added on the fly without impacting end users and without requiring re-provisioning.
- Call Server
  - ➢ Provides complete endpoint registration and call routing services for both H.323 and SIP protocols. It also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to transition to SIP in a gradual, orderly, and cost-effective manner.
  - ➢ Provides bandwidth management, and can be integrated with a Juniper Networks Session and Resource Control Module (SRC) to provide bandwidth assurance services.
  - ➢ Comes with a default dial plan that covers many common scenarios, but which can easily be modified.

The Call Server makes it possible for multiple UC environments and different video conferencing technologies to be unified across the network into a single dial plan.

See the *Polycom DMA 7000 System Operations Guide* for more information.

This section includes the following topics that discuss some of the considerations when integrating a DMA system with your RealPresence Resource Manager system.

- NTP Servers
- SIP Endpoint Management on page 264
- Conference Types Supported By the DMA System on page 264
- Considerations for Site Topology on page 265
- Scheduling Capacity on page 265
- Integrating with a DMA Supercluster

NTP Servers

It's important that you configure the RealPresence Resource Manager system and the DMA system to use the same NTP server. This ensures that each has the same network time as the other and scheduled conferences start when intended.

SIP Endpoint Management

For SIP-only endpoints that register with the DMA system and do not register with the RealPresence Resource Manager system's provisioning service, you must manually add them to the RealPresence Resource Manager system in order to manage that endpoint.

H.323 endpoints that register with the DMA system's gatekeeper automatically display in a RealPresence Resource Manager system that has been configured with a DMA system.

MCU Management

- When your system integrates with a Polycom DMA system, make sure the names of MCU systems that are managed by the RealPresence Resource Manager system includes a qualifier that indicates to the DMA system administrator that the MCU is directly registered to the RealPresence Resource Manager system; for example, ***ResourceManager_RMX10***.
- An RMX system can be managed by the RealPresence Resource Manager system or the Polycom DMA system, not both.

Conference Types Supported By the DMA System

You need to integrate with a Polycom DMA system in order to support the following RealPresence Resource Manager system conference types:

- **Anytime Conferences** are conferences that are initiated when the conference owner dials in and where most other participants are dial-out participants. Conference templates for anytime conferences are created and maintained on the DMA system.
- **Pooled Conferences** are conferences that are scheduled on resources managed by the Polycom DMA system. Conference templates for pooled conferences are created and maintained on the DMA system.

DMA Conference Templates

You need to have created DMA conference templates for schedulers to use when scheduling either a pooled conference (future) or anytime conference. You do this in the DMA system.

As a best practice, use a naming convention that helps identify the appropriate use for the conference template. For example, you can name conference templates intended for anytime conferences with an “anytime” prefix such as **anytime_corptemplate**.

Multi-Tenancy Considerations

DMA system conference templates are not area-aware, which means they cannot be associated with a particular area. An area scheduler can select any DMA system conference template to use for a conference.

As a best practice, you should use a naming convention that helps the scheduler identify the correct template to use for his area conferences.

Considerations for Site Topology

When integrated with the RealPresence Resource Manager system, the Polycom DMA system inherits site topology settings from the RealPresence Resource Manager system. Site topology configuration for both products is managed by a RealPresence Resource Manager system user with the administrator role.

When the RealPresence Resource Manager system is integrated with a DMA system, you should plan your site topology with DMA system needs in mind. For example, when your DMA system uses a supercluster environment, territories have specific functional roles. It’s important to work with your DMA system administrator to ensure the site topology meets your environments needs.

You should configure the Resource Manager Default territory to be the primary DMA node after you integrate with a DMA system.

See the *Polycom DMA 7000 System Operations Guide* for more information.

Scheduling Capacity

You can tune the scheduling capacity of the DMA system that the RealPresence Resource Manager system relies on. You do this through the RealPresence Resource Manager system.

The number of ports used for a conference can vary according to the MCU that hosts the conference and the number/type of endpoints that join. Because schedulers can only choose from a pre-configured DMA system pool order when scheduling pooled conferences, they rely on an administrator to tune the DMA system’s scheduling capacity to ensure efficient use of resources.

There are three ways an administrator can assess DMA system scheduling capacity:

- View conference reports from the DMA system. This method is preferred and provides the most accurate information.
- Monitor ongoing conferences to assess if resources were underbooked.
- View information on RealPresence Resource Manager CDR reports to review ports used for individual conferences.

Polycom recommends setting the DMA system scheduling capacity more conservatively at first and then tuning for increased conference activity. See Edit a Polycom DMA System on page 268.

Integrating with a DMA Supercluster

You can integrate with a DMA system that is deployed as a supercluster that uses single-node clusters. Polycom does not support Integrating with a DMA superclustered system that uses dual-node clusters at this time.

Working with a Polycom DMA System

You can integrate your RealPresence Resource Manager system with a Polycom DMA system. This section includes these topics:

- DMA View on page 266
- Add a Polycom DMA System on page 267
- Edit a Polycom DMA System on page 268
- Delete a Polycom DMA System on page 268

DMA View

Use the **DMA View** to view Polycom DMA systems v5.0 or later. You can integrate your RealPresence Resource Manager system with these later versions of the DMA system for both call server (gatekeeper and SIP proxy/registrar) and MCU pool order capability.

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

Field	Description
DMA Name	A unique name for the DMA system.
Description	A useful description for the Polycom DMA system.
IP Address/Hostname	The virtual IP address or FQDN for the DMA system. For DMA systems with multiple clusters, indicate the FQDN of the cluster you want to use. This FQDN or IP must be within the Call Server Sub-Domain defined in the DMA system. If your DMA system is configured for a super cluster, be sure to use the Virtual IP address for a cluster that is co-located with the RealPresence Resource Manager system.
Port	The port used to access the DMA system. The default port is **8443**.
MCU Pool Orders	A check mark displays if the DMA system has been enabled for MCU pool orders (conference management).
Call Server	A check mark displays if the DMA system has been enabled for use as a call server (gatekeeper).

Field	Description
Scheduling Capacity	The percentage of available ports to schedule for this DMA System.
Support DMA Super Cluster	Mark this box if your DMA system has been deployed as a supercluster. You must check this box if you want the RealPresence Resource Manager system to take advantage of the DMA's failover system and integrate with a backup DMA cluster if the primary DMA cluster goes down. If you mark this check box, you must also specify a Call Server Sub-Domain.
DMA Delegation Domain	Enter the FQDN of the Call server sub-domain controlled by the DMA system. The call server sub-domain is configured on the DMA system when the embedded DNS service is enabled. For example, `callservers.example.com`. See the Polycom DMA System Operations Guide for more information.

Add a Polycom DMA System

RealPresence Resource Manager system users with the Device Administrator role can add a Polycom DMA system to a RealPresence Resource Manager system.

- Before adding a Polycom DMA system to your RealPresence Resource Manager system, be sure that the DMA system is reachable via ICMP.
- You should configure the Resource Manager Default territory to be the primary DMA node AFTER you integrate with a DMA system.

To add a Polycom DMA system

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

2 In the **Add DMA** dialog box, enter a unique and identifying **Name** and **Description** for the DMA system.

3 Enter the **IP Address/Host** name. This field can be either the Virtual IP address of the DMA system or the DNS host name (FQDN).

For DMA systems with multiple clusters, indicate the FQDN of the cluster you want to use.

4 Enter the **Port** used to access the DMA system. The default port is **8443**.

5 Enter the **Username** and **Password** for the DMA system.

The DMA system user you use to authenticate the DMA system must have the Administrator role and gold class of service.

6 Mark the applicable check boxes in the **Used As** field.

You can use your DMA system as both of the following:

➢ a **Call Server** (gatekeeper)

➢ a conference manager **(MCU Pool Orders)**

7. Define the **Scheduling Capacity** as a percentage of total capacity.

   For more information about scheduling capacity, see Scheduling Capacity on page 265.

8. Mark the **Support DMA Supercluster** check box if your DMA system is deployed as a supercluster and you want the RealPresence Resource Manager system to integrate with the backup DMA cluster if a DMA system failover occurs.
9. If you marked the Support DMA Supercluster check box, you must also indicate a **DMA Delegation Domain**, see DMA View on page 266.
10. Click **Add**.

    The DMA system appears in the **Network Device** list.

    You should configure the Resource Manager Default territory to be the primary DMA node AFTER you integrate with a DMA system. For more information, see Territories on page 376.

Edit a Polycom DMA System

You must have the Device Administrator role in order to edit a Polycom DMA system.

To edit a DMA system

1. Go to **Network Device > DMA**.
2. Select the DMA system and click **Edit**.
3. In the **Edit DMA** dialog box, edit the properties of the DMA system.
4. Click **OK**.

Delete a Polycom DMA System

You must have the Device Administrator role in order to delete a Polycom DMA system.

To delete a DMA system from a RealPresence Resource Manager system

1. Go to **Network Device > DMA**.
2. Select the DMA system and click **Delete**.
3. Click **Yes** to confirm the deletion.

Managing DMA Pool Orders

When the RealPresence Resource Manager system is configured to work with a Polycom DMA system, conference schedulers can schedule conferences on DMA system pool orders.

DMA system pool orders associated with your configured DMA system are automatically displayed in the RealPresence Resource Manager system.

The DMA system administrator is responsible for setting up pool orders to be used. You should work with your DMA system administrator to determine the specifics about the pool orders associated with your DMA system. This information can also be useful for schedulers who need to choose a pool order to use for a conference.

DMA Pool Orders are groups of MCU pools that are hierarchically organized. Some uses for DMA system pool orders:

- The DMA system administrator can put all MCUs in a specific site or domain into a pool. Then, assign a pool order to all users in that site or domain (via group membership) ensuring that their conferences are preferentially routed to MCUs in that pool.
- The DMA system administrator could put one or more MCUs into a pool to be used only by executives, and put that pool into a pool order associated only with those executives' conference rooms.
- The DMA system administrator could put MCUs with special capabilities into a pool, and put that pool into a pool order associated only with custom conference rooms requiring those capabilities.

For more information about pool orders, see the *Polycom DMA 7000 System Operations Guide*.

This section includes the following topics:

- View Details of a DMA System Pool Order
- Associate a Polycom DMA System Pool Order with an Area

View Details of a DMA System Pool Order

You can use the RealPresence Resource Manager system to view DMA system Pool Order details. You cannot modify these properties. DMA system pool orders are created on the DMA system by a DMA system administrator.

To view details a DMA System Pool Order

1 Go to **Network Device > DMA Pool Orders.**

2 Select the DMA system pool order of interest.

The **DMA Pool Order Detail** pane is populated with the details for the selected pool order. These details are configured on the DMA system and cannot be modified with the RealPresence Resource Manager system.

Column	Description
Name	The unique name to identify the DMA System Pool Order.
Actual Capacity	The total number of ports included in this DMA System Pool Order.
Scheduling Capacity	The number of ports available to schedule for this DMA System Pool Order. This number matches the scheduling capacity percentage that was configured for this DMA system. Only users with the Device Administrator role can modify the scheduling capacity of a DMA system.

Associate a Polycom DMA System Pool Order with an Area

Users with Device Administrator role can associate a DMA pool order with an area.

When you do this, only schedulers belonging to that area can schedule conferences for that DMA system pool order. The advanced scheduler or area operator must either be in the same area as the DMA system pool order or be able to manage the area in which the DMA system pool order resides.

Schedulers and area schedulers cannot select particular resources on which to schedule conferences.

To associate a DMA System Pool Order with an Area

1. Go to **Network Device > DMA Pool Orders.**
2. Select the **DMA Pool Order** of interest and click **Associate Areas**.
3. In the **Available Areas** section, select and move the desired area(s) to **Selected Areas** list. You can move the unwanted are(s) to the **Available Areas** list. Press Shift-click or Ctrl-click to select multiple items in the list.

   You must have the Device Administrator role to associate a DMA system pool order with an area. The **Available Areas** list is limited to the areas that you manage.
4. Click **OK**.

Managing Border Controllers and Firewalls

This chapter describes how to perform the Polycom® RealPresence® Resource Manager system network device management tasks. It includes:

Manage Polycom VBP Devices

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

VBP View

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

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

The Polycom VBP 5300 or 6400 S/T platform has an access proxy feature that provides firewall traversal that enables the RealPresence Resource Manager system dynamic management features across a firewall.

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

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

Add a Polycom VBP Device

To add a Polycom VBP device to a RealPresence Resource Manager system

1. Go to **Network Device > VBPs** and click **Add**.
2. Configure these settings in the **Add VBP** dialog box.

Column	Description
Name	A unique name to identify the Polycom VBP device.
Provider-side IP	The Private Network IP address for the Polycom VBP device.
Subscriber-side IP	The Public Network IP address for the Polycom VBP device.

3. Click **OK**.

   A system dialog box appears indicating that you must restart Apache for the settings to take affect. You also have the opportunity to add another Polycom VBP device.

   The Polycom VBP device is added to the RealPresence Resource Manager system. However, more configuration may be necessary for the device to operate in your network. For example, you will probably need to Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device on page 272 as described in the next topic.

Copy the RealPresence Resource Manager System Certificate to a Polycom VBP Device

To copy the RealPresence Resource Manager system certificate to a Polycom VBP device

1. Go to **Network Device > VBPs**
2. Select the Polycom VBP device of interest and click **Copy Certificate to VBP**.

   In the **Copy Certificate to VBP** dialog box, the system automatically populates the **Filename** field with the filename of the RealPresence Resource Manager system certificate and the **Username** field with root.
3. Enter the SSH or console **Password** for the root user and click **OK**.

   The Polycom VBP device appears in the **Network Device** list.

Edit a Polycom VBP Device

To edit a Polycom VBP device

1. Go to **Network Device > VBPs**
2. Select the Polycom VBP device of interest and click **Edit**.
3. Configure these settings as needed in the **Edit VBP** dialog box.
4. Click **OK**.

Delete a Polycom VBP Device

To delete a Polycom VBP device from a RealPresence Resource Manager system

1. Go to **Network Device > VBPs**.
2. Select the Polycom VBP device of interest and click **Delete**.
3. Click **Yes** to confirm the deletion.

Identify Endpoints Using the Polycom VBP Device

This procedure identifies only Polycom HDX, Polycom Group, CMA Desktop, RealPresence Mobile, RealPresence Desktop and Polycom VVX systems that are:

- Registered to the RealPresence Resource Manager system
- Using the Polycom VBP firewall
- Use the RealPresence Resource Manager system as their provisioning server.

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

To identify which endpoints are using the Polycom VBP firewall

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

   The **Endpoint** list displays the dynamically-managed endpoints that are registered to the RealPresence Resource Manager system and using the Polycom VBP firewall. All of the endpoints display the same IP address, which is the Provider-side IP address of the Polycom VBP device. However, the endpoints will have different aliases and owners.

Dynamically Managing a Polycom RealPresence Access Director System

With the RealPresence Access Director system, Polycom offers a software-based edge server to securely route communication, management, and content through firewalls without requiring special dialing methods or additional client hardware or software.

Polycom supports dynamically managing or manually adding the RealPresence Access Director system.

When you manually add a RealPresence Access Director to your system, you will not be able to monitor its status or view any call information for calls routed from the RealPresence Access Director system.

> When you use the RealPresence Resource Manager system to dynamically manage a RealPresence Access Director system, you do not need to manually add it to your system.

For information about dynamically managing a RealPresence Access Directory system, see Dynamically Managing a RealPresence Access Director System on page 241.

Manually Add a RealPresence Access Director System

If you are not going to dynamically manage the RealPresence Access Director system, you can manually add it to the RealPresence Resource Manager system.

When you manually add a RealPresence Access Director system, you will not be able to monitor its status or view any call information for calls routed from the RealPresence Access Director system.

> When you use the RealPresence Resource Manager system to dynamically manage a RealPresence Access Director system, you should not manually add it to your system.

To manually add a RealPresence Access Director device to a RealPresence Resource Manager system

1 You should create a site that includes the subnet on which the RealPresence Access Director system resides.

See Add a Site on page 379.

> You cannot use the same site for more than one RealPresence Access Director system. You must create a unique site for each RealPresence Access Directory system that you use.

2 Go to **Network Device > RPADs** and click **Add**.

3 Configure these settings in the **Add RPAD** dialog box.

Field	Description
Name	A unique name to identify the RealPresence Access Director system.
IP Address	The Private Network IP address for the RealPresence Access Director system.

4 Click **OK**.

The RealPresence Access Director system is added to the RealPresence Resource Manager system. However, you will need to configure it more for the device to operate in your network. For more information, see the RealPresence Access Director system documentation.

Manage SBC Devices

Polycom supports the use of the Acme Packet Net-Net Enterprise Session Director session border control with the RealPresence Resource Manager system.

The SBC device management operations include these topics:

- Add a SBC Device
- Edit a SBC Device
- Delete an SBC Device
- Identify Endpoints Using the SBC Device

Add a SBC Device

Polycom supports the use of the Acme Packet Net-Net Enterprise Session Director session border control with the RealPresence Resource Manager system.

To add a SBC device to a RealPresence Resource Manager system

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

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

Field	Description
Name	A unique name to identify the SBC.
Provider-side IP	The Private Network IP address for the SBC device.
Subscriber-side IP	The Public Network IP address for the SBC device.

3 Click **OK**.

The SBC device is added to the RealPresence Resource Manager system. However, more configuration may be necessary for the device to operate in your network.

You also have the opportunity to add another SBC device.

Edit a SBC Device

To edit a SBC device

1. Go to **Network Device > SBCs**.
2. Select the SBC device of interest and click **Edit**.
3. Configure these settings as needed in the **Edit SBC** dialog box.
4. Click **OK**.

Delete an SBC Device

To delete a SBC device from a RealPresence Resource Manager system

1. Go to **Network Device > SBCs**.
2. Select the SBC device of interest and click **Delete**.
3. Click **Yes** to confirm the deletion.

Identify Endpoints Using the SBC Device

> This procedure identifies only Polycom HDX systems, Polycom Group systems and RealPresence Mobile clients that are:
>
> - Dynamically-managed by the RealPresence Resource Manager system
> - Using the SBC device

To identify which endpoints are using the SBC firewall

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

The **Endpoint** list displays the dynamically-managed endpoints that are registered to the RealPresence Resource Manager system and using the SBC firewall. All of the endpoints display the same IP address, which is the Provider-side IP address of the SBC device. However, the endpoints will have different aliases and owners.

User Management

This section provides an introduction to the Polycom® RealPresence® Resource Manager system video user management options functionality and operations. It includes:

Understanding Users, Groups, and Roles

The Polycom® RealPresence® Resource Manager system supports two types of users.

- Users that come directly from the enterprise directory. These users are referred to as **enterprise users.**
- Users that are local to the management system. These users are added manually to the system or imported.

Both user types can be assigned management roles, associated with endpoints, and organized in groups.

By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system users and groups management structure. It includes these topics:

- Working with Users on page 278
- Working with Groups on page 280
- Working with Management Roles and Permissions on page 281

Working with Users

The RealPresence Resource Manager system supports two types of users.

- Users that come directly from the enterprise directory. These users are referred to as **enterprise users.**
- Users that are local to the management system. These users are added manually to the system or imported from a file.

Local Users

When you manually add local users (or import them), the RealPresence Resource Manager system manages all user information and associations.

At a minimum, when you manually add users, you must enter a user’s **First Name** or **Last Name**, **User ID**, **Email Address**, and **Password**. When you enter the minimum information, the RealPresence Resource Manager system automatically assigns local users the basic **Scheduler** role or **Area Scheduler** role (when areas are enabled), unless you remove that assignment. You can unassign that role if the user does not need any management permissions.

By default all users can be scheduled into conferences, and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

You can associate local users with one or more roles and associate them with one or more endpoints. Alternatively, you can associate local users with roles by associating them with local groups, see Local Groups on page 280

If your company has implemented multi-tenancy, you can also associate local users with areas for which you manage. For more information about areas, see Configuring Multi-Tenancy on page 428 or Managing Areas on page 439.

Enterprise Users

When the RealPresence Resource Manager system is integrated with an enterprise directory, the system manages only the following pieces of an enterprise users' information:

- Endpoints associated with the user
- Roles assigned to the user
- Area to which the user belongs
- Alert profiles for the user

The remaining information is pulled from the enterprise directory, including E-mail address, system password and so on.

- Currently, the RealPresence Resource Manager system supports only a Microsoft Active Directory implementation of an LDAP directory.
- The RealPresence Resource Manager system displays a user's **City**, **Title**, and **Department** to help distinguish between users with the same name.

Users imported into the system through the enterprise directory are by default added to the system without a role. This default set up allows users to log into the RealPresence Resource Manager system with their enterprise user IDs and passwords. They can then be scheduled into conferences and call into conferences. However, the system cannot call out to them until they are associated with endpoints.

Assign Roles to Enterprise Users

You must decide which users will have management roles. Users with management roles can perform tasks on the RealPresence Resource Manager system, such as device management or conference scheduling. Management roles can be system-wide or area-restricted. A user must be assigned a management role in order to access the management system interface.

Conference participant users can be scheduled into conferences do not need to be assigned a management role, unless that particular user also needs to perform system management tasks.

If your company has implemented the Areas feature, you can also associate enterprise users with areas for which you are an administrator. For more information about areas, see Managing Areas on page 439 or Configuring Multi-Tenancy on page 428.

If you want the RealPresence Resource Manager system to, by default, to automatically assign enterprise users the basic **Scheduler** role, you must change the appropriate system **Security Settings**. See Give Enterprise Users Default Scheduler Role on page 327.

Working with Groups

Groups provide a more efficient and consistent use of the RealPresence Resource Manager system, because they allow you to assign roles and provisioning profiles to sets of users rather than to individual users.

This section includes the following topics:

- Local Groups on page 280
- Enterprise Groups on page 280

Local Groups

The RealPresence Resource Manager system allows you to add local groups (that is, groups added manually to the system) and associate them with provisioning profiles, roles and address books.

For local groups, the RealPresence Resource Manager system manages all group information and associations.

Enterprise Groups

When the RealPresence Resource Manager system is integrated with an enterprise directory, groups defined to the enterprise directory are not automatically added to the RealPresence Resource Manager system, but you can import them into the system.

When the RealPresence Resource Manager system is integrated with an enterprise directory, the system manages only three pieces of group information: the provisioning profile assigned to the group, the roles assigned to the group, and whether or not the group is Directory Viewable (that is, displayed in endpoint directories) or included in an address book. The remaining group information is pulled from the enterprise directory.

Prepare to Use Active Directory

To take full advantage of the RealPresence Resource Manager system, the enterprise Microsoft Active Directory must:

- Have Global Catalog turned ON. The Global Catalog enables searching for Active Directory objects in any domain without the need for subordinate referrals, and users can find objects of interest quickly without having to know what domain holds the object.
- Use universal groups. The Global Catalog stores the member attributes of universal groups only. It does not store local or global group attributes.
- Have a login account that has read access to all domains in the Active Directory that the RealPresence Resource Manager system can use. We recommend an account with a administrative username and a non-expiring password.

- Have the Active Directory Domain Name Service correctly configured. For more information about Active Directory design and deployment, see the Microsoft best practices guides at http://technet.microsoft.com.

For system and endpoint directory performance purposes, two best practices in regards to enterprise groups are:

- Do not import more than 500 enterprise groups into a RealPresence Resource Manager system.
- Do not mark more than 200 enterprise groups as **Directory Viewable**.

Working with Management Roles and Permissions

You must decide which users will have management roles. Users with management roles can perform tasks on the RealPresence Resource Manager system, such as device management or conference scheduling. Management roles can be system-wide or area-restricted. A user must be assigned a management role in order to access the management system interface.

Participant users who can be scheduled into conferences do not need to be assigned a management role, unless that particular user also needs to perform system management tasks.

For more information about area roles, see User Roles within a Multi-Tenancy Environment on page 429.

This section includes the following topics:

- Understanding User Roles on page 281
- Default System Roles and Permissions on page 282
- Customized Roles and Responsibilities on page 288

Understanding User Roles

The RealPresence Resource Manager system is a role and permissions based system.

- Users can assigned one or more user roles either directly or through their group associations.
- User roles are assigned a set of permissions. The system comes with default roles for both system-wide and area management tasks.
- Users see only the pages and functions available to their roles and associated permissions. Permissions are cumulative, so users see all of the pages and functions assigned to all of their roles and associated permissions.

> - Users inherit roles from their parent groups—local or enterprise. They cannot inherit roles from groups more distantly removed—for example, from their grandparent groups.
> - The default role names are stored in the system database and are not localized into other languages. If you wish to localized their names into your language, edit the roles and enter new names for them.

- If your company has implemented the Areas feature, users are restricted to the manage resources in the areas they are assigned to manage, according to the role they are given.

While the RealPresence Resource Manager system allows businesses almost unlimited flexibility in defining roles, for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

An administrator has several options when implementing user roles.

1. Implement only the default user roles and keep the standard permissions assigned to these roles.
2. Implement only the default user roles but change the permissions assigned to these roles.

> To ensure RealPresence Resource Manager system access and stability, the default Administrator role cannot be deleted or edited.

3. Implement either option 1 or 2, but also create additional unique, workflow-driven user roles and determine which permissions to assign to those user roles.

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**.

Default System Roles and Permissions

The RealPresence Resource Manager system includes a default set of management roles. Roles are associated with a set of permissions that allow the user to perform certain management tasks. Users see only the menus, pages, and functions associated with their roles.

While the RealPresence Resource Manager system allows administrators almost unlimited flexibility in defining roles, for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities. Because users can be assigned multiple roles, and permissions are cumulative, your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

The following table identifies the default system roles. Each of these roles is discussed in more detail in the following sections:

- Scheduler Roles, Responsibilities, and Menus on page 285
- Operator Role, Responsibilities, and Menus on page 286

- Device Administrator Role, Responsibilities, and Menus on page 286
- Auditor Role, Responsibilities, and Menus on page 287
- Administrator Role, Responsibilities, and Menus on page 287

For information about area roles, see User Roles within a Multi-Tenancy Environment on page 429.

> The default role names are stored in the system database and are not localized into other languages. If you wish to localized the role names into your language, edit the roles and enter new names for them.

Role	Permissions
Scheduler	Schedule Conferences Scheduling Level = Basic **When areas are enabled:** View and/or modify all areas. Can perform role tasks in all areas.
Advanced Scheduler	Schedule Conferences Scheduling Level = Advanced **When areas are enabled:** View and/or modify all areas. Can perform role tasks in all areas.
View-Only Scheduler	Schedule Conferences Scheduling Level = View-Only **When areas are enabled:** View and/or modify all areas. Can perform role tasks in all areas.
Operator	Conference Operator Report Operator Troubleshooting Schedule Conferences Scheduling Level = Advanced **When areas are enabled:** View and/or modify all areas. Can perform role tasks in all areas.

Role	Permissions
Device Administrator	Add endpoints and network devices. Network Device Admin Assign Provisioning Profiles through scheduled management Schedule software updates for endpoints **When areas are enabled:** View and/or modify all areas. Place devices and endpoints in Areas
Administrator **Note** This role cannot be deleted or edited.	Directory Setup Topology Setup Conferencing Setup System Setup Network Device Monitor System Maintenance/Troubleshooting and Trace troubleshooting Create Provisioning Profiles Create Software Updates Network device admin **When areas are enabled:** Assign RealPresence Resource Manager users to manage areas Create areas Place Entities in areas View and/or modify all areas
Auditor	Auditor

Most users will also see these menu items:

Description
Settings. Click here to display a **Settings** dialog box with the following information: • **User Name** • **Remote Server** • **Software Version** • **Font Size** In this dialog box, you can also: • Change the font size used in your display of the RealPresence Resource Manager system web client interface. • Change your password, if you are a local system user.
Downloads. Click here to display the **Downloads** dialog box with the downloadable applications that are compatible with the RealPresence Resource Manager system. Downloadable applications include: • CMA Desktop client for PC or MAC (including the path to the application) • Polycom File Verification Utility

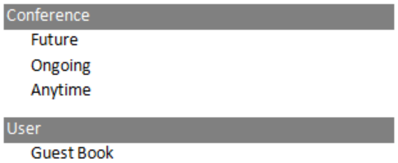
Description
Log Out. Click here to log out of the RealPresence Resource Manager system. **Note** The RealPresence Resource Manager system has an inactivity timer. If you are logged into the system but do not use the interface for a specified period of time (Five minutes by default), the system automatically logs you out.
Help. Links to the RealPresence Resource Manager system online help.

Scheduler Roles, Responsibilities, and Menus

The RealPresence Resource Manager system offers three different default **Scheduler** roles.

Role	Responsibilities
Scheduler	For the areas to which they belong (areas are optional), users assigned the **Scheduler** (sometimes called basic scheduler) role can schedule conferences. They do so using the conference templates defined for them. But basic schedulers cannot change any of the conference settings defined in the templates they choose when scheduling their conferences.
Advanced Scheduler	For the areas to which they belong (areas are optional), users assigned the **Advanced Scheduler** role can also schedule conferences. And again they do so using the conference templates defined for them. But advanced schedulers can change selected conference settings defined in the template they use when scheduling their conferences.
View-Only Scheduler	For the areas to which they belong (areas are optional), users assigned the **View-only Scheduler** role cannot schedule conferences; they can only see conferences that have been scheduled.

When basic or advanced schedulers log into the RealPresence Resource Manager system, the system displays the **Future** conference page and they have access to the following menu items:



When view-only schedulers log into the RealPresence Resource Manager system, the system displays the **Future** and **Ongoing** conference page and it is the only menu item to which they have access.

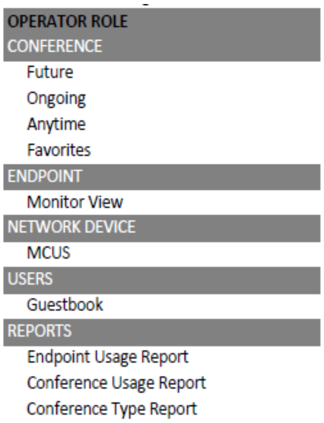
Operator Role, Responsibilities, and Menus

The **Operator** role allows businesses to offer high-touch customer service for video conferencing. User assigned the **Operator** role can:

- Schedule conferences.
- Monitor and manage ongoing conferences.

- Monitor endpoints.
- Monitor network devices such as MCUs.
- Add, edit, and delete entries in the system **Guest Book**.
- Create favorites.
- View some system reports.

When operators log into the RealPresence Resource Manager system, the system displays the **Ongoing** conference page and they have access to the following menu items:



OPERATOR ROLE

CONFERENCE

- Future
- Ongoing
- Anytime
- Favorites

ENDPOINT

- Monitor View

NETWORK DEVICE

- MCUS

USERS

- Guestbook

REPORTS

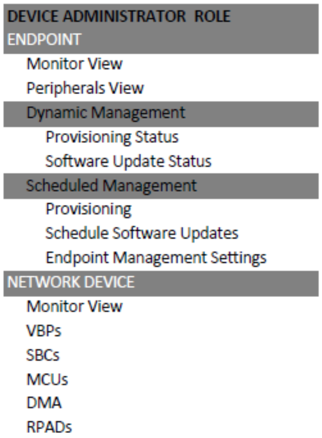
- Endpoint Usage Report
- Conference Usage Report
- Conference Type Report

Device Administrator Role, Responsibilities, and Menus

The Device Administrator role is for those users who administrate endpoints, bridges, and other network devices. For the areas to which they belong, users assigned the Device Administrator role can:

- Monitor endpoints, peripherals, and network devices.
- Add, edit, and delete endpoints and network devices.
- Provision endpoints using scheduled management.
- Update endpoints using scheduled management.

When device administrators log into the RealPresence Resource Manager system, the system displays the system Dashboard and they have access to the following menu items:



DEVICE ADMINISTRATOR ROLE

ENDPOINT

- Monitor View
- Peripherals View
- Dynamic Management
  - Provisioning Status
  - Software Update Status
- Scheduled Management
  - Provisioning
  - Schedule Software Updates
  - Endpoint Management Settings

NETWORK DEVICE

- Monitor View
- VBPs
- SBCs
- MCUs
- DMA
- RPADs

Auditor Role, Responsibilities, and Menus

The **Auditor** role allows security-conscious companies to separate system administration functions from system auditing functions. This provides an added level of system checks and balances. This role must be explicitly assigned by an administrator.

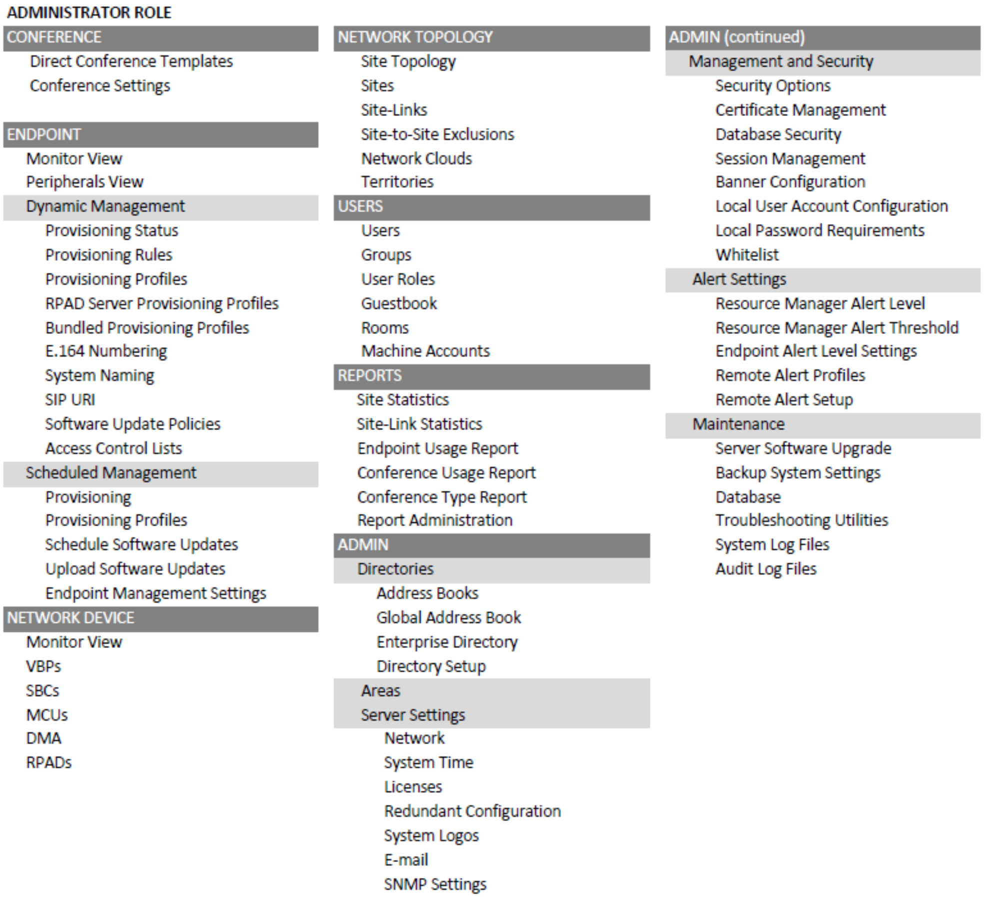
For the areas to which they belong, users assigned the **Auditor** role can:

- View audit logs.
- Backup and delete audit logs.
- Change the audit log file alert level.
- View and download system log files.
- Respond to audit log alerts.

Administrator Role, Responsibilities, and Menus

The **Administrator** role is for those users who administrate the RealPresence Resource Manager system itself. Users assigned the **Administrator** role can generally do almost all system functions, however they cannot schedule conferences, monitor conferences, or manage endpoints or other network devices.

When administrators log into the RealPresence Resource Manager system, the system displays the system **Dashboard** and they have access to the following menu items:



ADMINISTRATOR ROLE

- CONFERENCE
  - Direct Conference Templates
  - Conference Settings
- ENDPOINT
  - Monitor View
  - Peripherals View
  - Dynamic Management
    - Provisioning Status
    - Provisioning Rules
    - Provisioning Profiles
    - RPAD Server Provisioning Profiles
    - Bundled Provisioning Profiles
    - E.164 Numbering
    - System Naming
    - SIP URI
    - Software Update Policies
    - Access Control Lists
  - Scheduled Management
    - Provisioning
    - Provisioning Profiles
    - Schedule Software Updates
    - Upload Software Updates
    - Endpoint Management Settings
- NETWORK DEVICE
  - Monitor View
  - VBPs
  - SBCs
  - MCUs
  - DMA
  - RPADs
- NETWORK TOPOLOGY
  - Site Topology
  - Sites
  - Site-Links
  - Site-to-Site Exclusions
  - Network Clouds
  - Territories
- USERS
  - Users
  - Groups
  - User Roles
  - Guestbook
  - Rooms
  - Machine Accounts
- REPORTS
  - Site Statistics
  - Site-Link Statistics
  - Endpoint Usage Report
  - Conference Usage Report
  - Conference Type Report
  - Report Administration
- ADMIN
  - Directories
    - Address Books
    - Global Address Book
    - Enterprise Directory
    - Directory Setup
  - Areas
  - Server Settings
    - Network
    - System Time
    - Licenses
    - Redundant Configuration
    - System Logos
    - E-mail
    - SNMP Settings
- ADMIN (continued)
  - Management and Security
    - Security Options
    - Certificate Management
    - Database Security
    - Session Management
    - Banner Configuration
    - Local User Account Configuration
    - Local Password Requirements
    - Whitelist
  - Alert Settings
    - Resource Manager Alert Level
    - Resource Manager Alert Threshold
    - Endpoint Alert Level Settings
    - Remote Alert Profiles
    - Remote Alert Setup
  - Maintenance
    - Server Software Upgrade
    - Backup System Settings
    - Database
    - Troubleshooting Utilities
    - System Log Files
    - Audit Log Files

Customized Roles and Responsibilities

The RealPresence Resource Manager system allows you almost unlimited flexibility in defining and redefining roles, but for simplicity and clarity, we recommend keeping the default roles with their default permissions and responsibilities.

Users can be assigned multiple roles and permissions are cumulative, so your business can combine roles as needed to reflect the workload your people undertake to manage and use the system.

Managing Users

This chapter includes information on managing users and groups within the Polycom® Real Presence® Resource Manager system. It includes these topics:

Manage Users

In the RealPresence Resource Manager system, only users assigned the **Administrator** role can manage users. Some of these tasks include:

Search for a User

To search for a user

1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

2. To search for a local user, press **Enter**.
3. To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.

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

View User Information

You can view information about a user, local or enterprise.

To view the address book a user is assigned to

1. Go to **User > Users**.
2. Select the user you want.
3. Click **View Details**.

Column	Description
General Info	
First Name	The user’s first name.
Last Name	The user’s last name.
User ID	The user’s unique login name. This user ID must be unique across all rooms and users and across all domains.
Email Address	The user’s E-mail address. (The **Email** address is an ASCII-only field.)
Title	The user’s professional title.
Department	The user’s department within the enterprise.
City	The city in which the user’s office is located.
Phone Number	The contact phone number for the user.
Belongs to Area	This field is only available if Areas have been enabled.
Manages Area	This field is only available if Areas have been enabled.

Column	Description
Associated Roles	
Assigned Roles	The roles assigned to the user. For more information, see Working with Management Roles and Permissions on page 281.
Groups	
Type	The type of group to which the user belongs. Possible values are local and enterprise.
Name	The name of the group to which the user belongs.
Inherited Group Info	
Address Book	The Address Book(s) the user sees based upon the groups to which the user is assigned.

Add a Local User

To add a local user

1 Go to **User > Users** and click **Add**.

The **Add New User** dialog box appears. The **Enable User** option is selected by default.

2 Enter the following user information.

Column	Description
First Name	The user’s first name
Last Name	The user’s last name
User ID	The user’s unique login name. This user ID must be unique across all rooms and users and across all domains. **For Multi-Tenancy:** Create user names using the email address format. This will ensure that all user names are unique. Otherwise two people named Bob Smith belonging to different tenants may end up with the same user name. By following an email address format, Bob Smith in TenantA could have bsmith@tenantA.com as a user name and Bob Smith in TenantB could have bsmith@tenantB.com.
Password	The user’s assigned password. This password must be a minimum of eight characters in length.
Email Address	The user’s Email address. (The **Email** address is an ASCII-only field.)
Title	The user’s professional title.
Department	The user’s department within the enterprise.
City	The city in which the user’s office is located.

Column	Description
Phone Number	The contact phone number for the user.
Assign Area	If your RealPresence Resource Manager system has areas enabled, you can choose to assign this user to an area that you manage.

3 In the **Associated Endpoints** section, select and move the required endpoints(s) to **Selected Endpoints** list. Move the unwanted endpoints(s) to the **Available Endpoints** list. Press Shift-click or Ctrl-click to select multiple items in the list.

4 In the **Associated Roles** section, select and move the required role(s) to **Selected Roles** list. Move the unwanted role(s) to the **Available Roles** list. Press Shift-click or Ctrl-click to select multiple items in the list.

> If the user has multiple endpoints, list the endpoints in order of priority, with the primary endpoint first.

5 If Areas are enabled, click the **Managed Areas** section.

You must have either the administrator role or have the area administrator role and be allowed to manage more than one area in order to perform this action.

- If the user has not been assigned a role, select the **None** radio button and continue to the **Associated Alert Profile** section.
- If the user has been assigned an role, select the **Specific Areas** radio button.

6 In the **Available Areas** section, select and move the required area(s) to **Selected Areas** list. Move the unwanted role(s) to the **Available Areas** list. Press Shift-click or Ctrl-click to select multiple items in the list.

The user will be assigned to manage the areas in the **Selected Areas** section.

7 In the **Associated Alert Profile** section, select a **Remote Alert Notification Profile** as appropriate.

8 In the **SIP Dial String Reservations** section, select the user's **Device Type** and enter the appropriate dial string for **SIP URI**, then click **Apply**.

The dial strings appear in the list below.

By default, the same SIP URI is used for all endpoints that belong to the same user. If the user has multiple endpoints and you want a different SIP URI for each device type, enter the dial strings for one endpoint type at a time and click **Apply** each time.

9 In the **H323 Dial String Reservations** section, select the user's **Device Type** and enter the appropriate dial string for **E164** and **H323 ID**, then click **Apply**.

The dial strings appear in the list below.

If the user has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.

10. Click OK.

    If the **Phone Number** you entered is exactly the same as an existing user or endpoint, the **Phone Number Conflict** dialog box appears and lists the names of the other users or endpoints with the same number.

    - To keep the duplicate number, click **Continue**.
    - To change the phone number, click **Cancel**.

Edit a User

For local users added manually to the RealPresence Resource Manager system, you can edit all user information. If you change the user ID, the user must log into the associated endpoints with the new 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 endpoints, but you cannot change user names, user IDs, or passwords.

To edit a user

1. Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

> Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

2. To search for a local user, press **Enter**.
3. To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

> If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

4. If the list is too large to scan, further refine your search string.
5. Select the user of interest and click **Edit**.
6. As required, edit the **General Info**, **Associated Devices, Associated Roles, Managed Areas**, **Associated Alert Profile**, and **Dial String Reservations** sections of the **Edit User** dialog box.
7. Click OK.

View Role Information for a User

A user with the **Administrator** role or **Area Administrator** role can view role information for a user.

To view permissions a user

1. Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

> Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

2 To search for a local user, press **Enter**.

3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

> If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

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

5 Select the user of interest and click **View Details**.

The **Edit User** dialog box displays.

6 Click **Associated Roles** to view the role information for this user.

7 Click OK.

Delete a User

You can only delete local users from the RealPresence Resource Manager system. You cannot delete users added through integration with an enterprise directory.

To delete a user

1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest.

> Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

2 To search for a local user, press **Enter**.

3 To search both local and enterprise users, first clear the **Local Users Only** check box and then press **Enter**.

> If you are not in an enterprise domain, you will not have the option of searching for enterprise users.

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

5 Select the user of interest and click **Delete**.

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

The user is deleted from the Resource Manager system.

Unlock a User Account

When a local user reaches the **Failed login threshold**, the system will not allow the user to log in until an administrator unlocks the user’s account. When a user’s account is locked, the system will display an error message.

To unlock a user account

1 Go to **User > Users** and in the **Search Users** field, enter the name of the user of interest and press **Enter**.

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

3 Enable the **Unlock User** option and click **OK**.

The system should allow the user to log in.

Import Local Users

You can import local users into your RealPresence Resource Manager system. You may choose to do this if your RealPresence Resource Manager deployment does not include an integration with an LDAP server and you need the convenience of importing users in bulk instead of creating them one at a time.

You can only import a file when you are using Internet Explorer or Google Chrome as your browser.

Importing Users When Areas Are Enabled

You can only import users to one area at a time and must have either the administrator role or area administrator role in order to import users.

To import users to your system,

1 Create a CSV File Containing the User Information you need on page 296.

2 Import the CSV File on page 297.

3 Review the Import Details File on page 298.

Create a CSV File Containing the User Information you need

You must create a CSV (comma separated values) file that contains the users you need. You can create this file with any plain text editor or use Microsoft Excel.

When working on a double-byte system such as Chinese or Japanese, you need to ensure the .CSV file is encoded using UTF-8. CSV files created with Microsoft Excel do not support UTF-8 encoding. When exporting as CSV, you need to save the file first and then open it in an application that supports UTF-8 encoding. When importing, you need to be sure that the file has been saved with UTF-8 encoding. Polycom recommends using a tool such as NotePad ++ to save the CSV file using UTF-8 encoding.

The format should be the following:

```
Username, First Name, Last Name, Email, Title, Dept, City, Phone Number,
Role(s), Password
```

Use the following guidelines:

- Use a file with a *.csv extension.
- All fields for a single user must be on a single line and end with a new line or end of file character. The line after a new line is assumed to be for another user.
- Commas (‘,’) are used as field separators and cannot be embedded in a field. All commas must be included, even before fields that are optional. Each field’s leading and trailing white space (blanks and tabs) is ignored (does not become part of the field value).
- Unicode characters are allowed in the file as long as they are valid for the field type.
- Blank lines are allowed and are ignored.
- A header line is not allowed in the CSV file. All lines must either represent a user or be blank.
- The following fields are required: Username, First Name or Last Name, and Email.
- Other fields can be left blank, but not skipped.
- Be sure you are using Internet Explorer or Google Chrome as your browser.

Field	Usage Notes
Username	The username must be unique across the entire RealPresence Resource Manager system. (The recommended naming convention to ensure uniqueness is specified in section If a specified username already exists in the selected area (or in the system, if Areas is disabled), then the system assumes you wish to update the existing user’s information. If a specified username already exists in a different area, then the user is neither added nor updated and an error is issued.
Role(s)	Role names are case sensitive. To specify multiple roles for a user, separate the roles with a pipe (‘|’). If the Role(s) field contains only area-specific roles, then the user will automatically be set to manage the selected area.
Password	If any of the users have no password specified, then a single default password is generated and assigned to all those without a password specified. The administrator will be shown what password was assigned to all and is responsible for writing it down and communicating it to all the users. For users assigned default passwords, the first time they log in, they will be required to change their password.
Email	Be sure to includes a valid email address.

Examples

This first example shows all fields specified:

```
js@co.com, John, Smith, js@co.com, Tech I, IT, Boulder, 303-333-4444, Role
1|Role 2, JSpw
```

This example shows only the required fields specified. In this case, the user will be given a blank first name, title, department, city and phone number, no role and a generated password.

```
jdoe, , Doe, doe@co.com, ,  ,  ,scheduler,  ,
```

Import the CSV File

You need to have either the administrator or area administrator role to import users.

Note

The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To import local users to the RealPresence Resource Manager system

1. Choose **User > Users** and click **Import Local Users**.
2. In the **File Location (CSV)** field, browse to the location of the CSV file you created.
3. If areas are enabled and you manage more than one area, select an area from the **Assign Area** drop-down list.

Importing Users into an Area

If Areas are not enabled on your RealPresence Resource Manager system or you only manage one area, the Areas drop-down is not available.

If Areas are enabled and the you manage more than one area, you must select an area to which all the users will be added. You can also select None to add the users to no area.

4. Click **Import**.

   A status window appears. Click OK when it is complete.

   The results of the import are summarized on the Import Summary screen.

5. If a default password is shown in the summary, write the password down and inform those users of the password.

Default Passwords Created During Import

If you fail to record/remember the password shown on the Import Summary screen, there will be no other way to determine it and the users will be unable to login. If this happens, you can either:

- Edit each affected user one-by-one via the RealPresence Resource Manager system’s User Edit screen and manually change the password field or have system generate a password.
- Delete all affected users one-by-one via the RealPresence Resource Manager user interface and re-import them.

6. Click **Download Import Details** to view the import details file. Save it as a text file for your records.

7 Close the **Import Users** dialog box.

Review the Import Details File

You should review the Import Details file for any information about errors that may need to be corrected.

If there are errors, you can either:

- Create another CSV file with the users that need to be corrected and import only those users.
- Edit the same CSV file to correct the users with errors and import the file again. Users that were previously added successfully will be updated, see Updating Users by Import on page 299. Specifically, existing user updates will fail if a password is specified, so either remove those user's passwords or ignore password errors that are issued for those users who were previously added.

In either case, realize that a different default password will be assigned in subsequent imports than was assigned to users in a previous import.

> If there are errors and you do not view the Import Details file, you will not know what errors were issued or for which users.

Updating Users by Import

You can also use the Import Local Users action to update existing users.

The CSV format for updating an existing user is the same as that used for adding a user except that the password field must be blank. For each existing username whose attributes are to be updated, the CSV format is:

```
Username, First Name, Last Name, Email, Title, Dept, City, Phone Number,
Role(s),
```

Note that the comma after the Role(s) field is still required.

> Importing a CSV file that has existing usernames will overwrite existing data. Make sure the CSV data is at least as current as what is in RealPresence Resource Manager system. Determining existing user data can be done one-by-one and manually via the RealPresence Resource Manager system user interface (currently there is no way to export local user data in bulk).

A single CSV file may contain both users to be added and users to be updated. The system will automatically determine whether you are intending to add or update a user by whether the username already exists in the system or not:

The following fields cannot be changed using the Import Local Users action.

- An existing user's username
- An existing user's password
- Any of the attributes not specified in the Import CSV format

The following rules apply when updating existing users.

- The Username must already exist in the selected area.

  You can only change an existing user’s username by using the Resource Manager system user interface.

- The Password must be blank. If a password is specified, the update for that user will fail such that none of the fields will be updated.

  You cannot change a user’s password with an import. You must use the system’s web interface.

- Fields that are left blank will replace any existing data that the Resource Manager system has for that user with a blank.
- There is no way to indicate that any of the user’s data should be left as is.
- All other user attributes not included in the CSV format, such as which areas a user manages, will not be modified by an Import.

When importing double-byte characters such as Chinese or Japanese, you need to ensure the .CSV file is encoded using UTF-8. CSV files created with Microsoft Excel do not support UTF-8 encoding. Polycom recommends using a tool such as NotePad ++ to save the CSV file using UTF-8 encoding.

Add Machine Accounts

For dynamically managed endpoints associated with a room, a user assigned the **Administrator** role must associate each room in the RealPresence Resource Manager system with a machine account. In addition, dynamically managed HDX systems and RealPresence Group systems require machine accounts.

The machine account allows the endpoint to connect and authenticate with the RealPresence Resource Manager system for directory and dynamic management purposes without using the endpoint user’s account. You should use a unique machine account for each room or endpoint you need to provision.

You can set up the room and machine account the following ways:

- You can set up a machine account and create a new room at the same time, then edit the room to complete the room information.
- You can create a new room, then create the machine account and associate the machine account with the existing room. For more information, see Add a Local Room on page 319.
- If your system is integrated with Active Directory and you want to associate a machine account with an Active Directory account, you must first create that account in Active Directory.

To add a machine account

1. Go to **User > Machine Accounts**.
2. Click **Add**.
3. In the **Add Machine Account** dialog box, complete the fields.
4. Click **OK**.

The **Add Machine Account** dialog box includes the following information.

Field	Description
Enable Machine Account	Select or clear this option to enable and disable (respectively) the machine account you create for the endpoint.
Unlock Machine Account	Select this option to unlock machine accounts that become locked when they exceed the Failed login threshold. This will only happen when the password expires.
User ID	Enter a unique name for the machine account. As a best practice, name the machine account in a way that associates it with the corresponding device. For example, if your company names endpoint systems for the system user or room (for example, `bsmith_HDX` or `Evergreen_Room`), then give the machine account an associated **User ID** (`bsmith_HDX_machine` or `evergreen_room_machine`).
Password/ Confirm Password	Enter a password for the machine account user ID. This password must meet the **Local Password Requirements**. This password expires in 365 days.
Description	Enter a meaningful description for the endpoint.
Associate with an existing user or room	Select this option to associate the endpoint system with a specific user or room. This may be a local or enterprise user or room.
Associate with a new room (created automatically)	Select this option to associate the endpoint system with a system-generated room. The name of the new room is the same as the machine account **User Name** and can be edited when you edit the room. This option can only create a local room account. If you want to associate a machine account with an Active Directory account, you must first add the account through Active Directory.
Assign Area	When areas are enabled, you can assign the newly-created room to an area. Only users who manage more than one area can assign areas.

Once you have created this machine account on the RealPresence Resource Manager system, provide this information to the appropriate endpoint administrator. They should enter this **User ID** and **Password** as the **User Name** and **Password** on the **Provisioning Service** page.

Note that the machine account password expires after one year. After the expiration, the endpoint login will fail. After three failed login attempts, the system locks the machine account. You can reset the password and unlock the machine account by editing it and assigning a new password.

Manage Dial String Reservations for Users

If you need to make multiple dial string reservations for multiple users, you can use the **Import User Alias** function. If you need to make a report of which dial strings (H.323 or SIP URIs) have been reserved for each user, you can use the **Export User Alias** function.

Both the **Import User Alias** and **Export User Alias** features allow you to manage the dial string reservations for all users at once. If you need to only add or modify a dial string for a single user, it is more efficient to edit that user's dial strings directly, see Edit a User on page 293.

Dial string reservations take first priority when they are associated with a user and will overwrite any provisioned H.323 alias or SIP URI for that user.

Specifically, SIP URI dial string reservations are assigned in the following three ways, listed by priority:

1. Dial string reservation associated with user record.
2. Domain user or third-party server (for example, Microsoft Lync)
3. Auto-generated SIP URI through the RealPresence Resource Manager system

Exporting User Aliases

You can export a report of users with reserved SIP URI aliases, either SIP or H.323. Keep in mind that this CSV file will contain displays reserved aliases and dynamically-provisioned aliases if the provisioning information has already been sent.

> **Exporting Alias Information When Areas Are Enabled**
> Users with the area administrator role can only export aliases from one area at a time or from only the areas they manage. Users with the administrator role can export alias information from all areas.

To export a list of user aliases

1. Navigate to **User > Users**.
2. Click **Export User Aliases** in the Actions list.
3. In the **Export User Aliases** dialog box, mark **SIP URI** aliases and click **Export**.

   You cannot export both H.323 and SIP aliases in the same report. You must export them separately.
4. Save the report.

Importing User Aliases

You can import a list of user aliases that will add to or overwrite any existing reserved dial string aliases that have been associated with users.

You will need to create a CSV (comma separated values) file that lists the user information and user alias reservations you wish to add or update. You may use any text editor or Microsoft Excel to create the CSV file.

> When working on a double-byte system such as Chinese or Japanese, you need to ensure the .CSV file is encoded using UTF-8. CSV files created with Microsoft Excel do not support UTF-8 encoding. When exporting as CSV, you need to save the file first and then open it in an application that supports UTF-8 encoding. When importing, you need to be sure that the file has been saved with UTF-8 encoding. Polycom recommends using a tool such as NotePad ++ to save the CSV file using UTF-8 encoding.

Use the following guidelines:

- Use a file with a *.csv extension.
- All fields for a single user must be on a single line and end with a new line or end of file character. The line after a new line is assumed to be for another user.
- Commas (‘,’) are used as field separators and cannot be embedded in a field. All commas must be included, even before fields that are optional. Each field’s leading and trailing white space (blanks and tabs) is ignored (does not become part of the field value).
- Unicode characters are allowed in the file as long as they are valid for the field type.
- Blank lines are allowed and are ignored.
- A header line is not allowed in the CSV file. All lines must either represent a user or be blank.

Note

The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

SIP Format:

```
Domain, username, device type, SIP URI, Device Name
```

Where:

Commas (‘,’) are used as field separators and cannot be embedded in a field. The device name should be used if you need to differentiate between two device names (HDX1 and HDX1) of the same device type for the same user. The device name is required in order to associate the SIP URI with a device. You do not need to include a SIP URI for all users in the file, but at least one user must have a value for the SIP URI field.

The following fields are required: Domain, Username, **Device Type** and **SIP URI**.

Other fields can be left blank, but not skipped.

Field	Usage Notes
Domain	Specifies the domain of the user.
Username	The username must already exist in the RealPresence Resource Manager system. This can be the user ID of a user or a machine account, or the name of a room.
Device Type	The following are valid device types: HDX VVX CMADesktop RPMobile GroupSeries RPDesktop All_Types

Field	Usage Notes
URI	The SIP URI for this user. The SIP URI supports alphanumeric characters and the following special characters: '.', '-', '_', '@', ':'.
Device Name	The device name should be included if you need to differentiate between two device names (jsmithHDX1 and jsmithHDX2) for the same device type for the same user.

Examples

- This first example reserves the SIP URI to all device types for this user:

  ```
  local,johndoe,All_Types,johndoe@example.com
  ```

- This example reserves the SIP URI to the HDX for this user.

  ```
  local,johndoe,HDX,johndoeHDX@example.com
  ```

- This example reserves the SIP URI to the HDX that is named johndoeHDX2.

  ```
  local,johndoe,HDX,johndoeHDX2@example.com,johndoeHDX2
  ```

H323 Format

```
Domain, Username, Device Type, H.323 ID, E.164 Number, Device Name
```

Where:

Commas (‘,’) are used as field separators and cannot be embedded in a field. The device name should be used if you need to differentiate between two device types (HDX1 and HDX1) of the same type for the same user. You can supply an H.323 ID, an E.164 number or both. You do not need to enter a dial string for each user in the file.

The following fields are required: Domain, Username, **Device Type, H323 ID** and **E.164**.

Other fields can be left blank, but not skipped.

Field	Usage Notes
Domain	Specifies the domain of the user.
Username	The username must already exist in the RealPresence Resource Manager system. This can be the user ID of a user or a machine account, or the name of a room.
Device Type	The following are valid device types: HDX VVX CMADesktop RPMobile GroupSeries RPDesktop
H.323 ID	The H.323 ID for this user. The H.323 ID supports alphanumeric characters and the following special characters: '.', '-', '_', '@', ':'.

Field	Usage Notes
E.164 Number	The E.164 number for this user. The E.164 number must consist of only numeric characters.
Device Name	The device name should be included if you need to differentiate between two device names (jsmithHDX1 and jsmithHDX2) for the same device type for the same user. The device name is required if you want to associate the SIP URI with a particular device name that has been assigned to a user.

Examples

- This first example reserves the H.323 ID and E.164 number for this user's HDX system.

  ```
  local,johndoe,HDX,johndoeHDX,771000
  ```

- This example updates the H.323 ID and E.164 number for this user's "johndoeHDX2".

  ```
  local,johndoe,HDX,johndoeHDX2,771001
  ```

To import a list of user aliases

1. Create a valid CSV file to use. It may be helpful to use an exported User Alias CSV file on which to base your changes.
2. Navigate to **User > Users**.
3. Click **Import User Aliases** in the Actions list.
4. In the **Import User Aliases** dialog box, mark **SIP URI** aliases or **H323** aliases and click **Export**.

   You cannot import both H.323 and SIP aliases in the same report. You must export them separately.
5. Click **Update.**

   An error message will display if your CSV file contained any mistakes. If you get an error message, you will need to correct the rows that were not loaded and import them again.

Manage Groups

In the RealPresence Resource Manager system, only users assigned the **Administrator** role can:

- Add a Local Group on page 305
- Import Enterprise Groups on page 306
- Edit a Group on page 307
- Delete a Group on page 307

Add a Local Group

To add a local group

1. Go to **User > Groups**.

2 In the **Groups** page, click **Add Local Group**.

3 Complete the **General Info** section of the **Add Local Group** dialog box.

Column	Description
General Info	
Group Name	A meaningful and unique group name assigned when creating the group.
Description	A more complete description of the group's purpose
Directory Viewable	Whether or not the group is displayed in the endpoint directory
Address Book	See Assign Address Books to Groups on page 424.
Assigned Area	If your RealPresence Resource Manager system has areas enabled, you can choose to assign this user to an area that you manage,.
Associated Roles	
Available Roles	The list of roles defined to the RealPresence Resource Manager system.
Selected Roles	The list of roles that you assign users when adding them to the system. Users have all of the permissions associated with all of the roles assigned to them (that is, permissions are cumulative).
Group Members (Local Users Only)	
Search Available Members	Search field for finding users
Search Results	The users and groups identified to the system that you can add to the local group. This list can include both local and enterprise users and groups.
Group Members	The users and groups selected as part of the group

4 In the **Search Available Members** field of the **Group Members** dialog box, search for the users and groups to add to this local group.

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 check box in the column header.

6 Click **OK**.

The group appears in the **Groups** list. It is identified as a LOCAL group.

Import Enterprise Groups

To import one or more enterprise groups

1 Go to **User > Groups**.

2 In the **Groups** page, click **Import Enterprise Group**.

3 In the **Search Available Groups** field of the **Import Enterprise Group** dialog box, type all or part of the group name (with wildcards) and press ENTER.

Searches for a group are case-insensitive, exact-match searches of the **Group Name** field. Use wildcard characters to perform substring searches.

4 In the **Search Results** list, select the enterprise groups to add. To select all enterprise groups, click the check box 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, user roles, and specify whether or not the group directory is viewable. You can also search for enterprise users.

Edit a Group

To edit a local or enterprise group

1 Go to **User > Groups**.

2 In the **Groups** page, select the group of interest and click **Edit**.

3 As required, edit the **General Info**, **Associated Roles,** and **Group Members** sections of the **Edit Local Groups** dialog box.

- The **Group Members** section is only available for Local groups.
- If you remove a user from a group or a role from a group, the user no longer has the roles associated with the group.

4 Click OK.

Delete a Group

To delete a local or enterprise group

1 Go to **User > Groups**.

2 In the **Groups** page, select the group of interest and click **Delete Group**.

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

The group is deleted from the system.

An enterprise group is only deleted from the system, not the enterprise directory, so it can be re-imported.

Manage User Roles

In the RealPresence Resource Manager system, only users assigned the **Administrator** role can:

- Assign Users Roles and Endpoints on page 308
- View the List of User Roles on page 308
- Add a User Role on page 308
- Edit Permissions for a User Role on page 309
- Delete a User Role on page 310
- View the Groups and Users Associated with a User Role on page 310

Assign Users Roles and Endpoints

You can assign roles to both local and enterprise users and associate them with endpoints.

To assign a role and endpoint to a user

1 Go to **User > Users**.

2 To search for a user:

a In the **Search** field of the **Users** page, type a search string.

> Searches for a user on the RealPresence Resource Manager system **Users** page are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

b To search both local and enterprise users, clear the **Local Users Only** check box and press **Enter**.

The first 500 users in the database that match your search criteria are displayed in the **Users** list.

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

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

4 In the **Devices** section of the **Edit User** dialog box, select the endpoint to associate with the user and move it to the **Selected Devices** column. If a user has multiple endpoints, the first endpoint listed is the user’s default endpoint.

5 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.

6 Click Finish.

View the List of User Roles

To view the list of User Roles

» Go to **User > User Roles**.

The **User Roles** list appears. It can be filtered by **Name** and **Description**.

Column	Description
Name	The unique name of the user role
Description	An optional description of the role

Add a User Role

When you add a user role, you also specify permissions for the role.

To add a new user role

1 Go to **User > User Roles**.

2 On the **User Roles** page, click **Add**.

3 Complete the **Name** and **Description** fields of the **Add Role** dialog box and assign permissions to the new role.

The following table describes the fields of the **Add Role** dialog box.

Field	Description
Name	The unique name (ASCII only) of the user role
Description	(Optional) A useful description (ASCII only) of the user role
Administrator Permissions	Identifies which RealPresence Resource Manager system administrator pages and functions are available to the user role.
Operator Permissions	Identifies which RealPresence Resource Manager system operator pages and functions are available to the user role.
Scheduler Permissions	Identifies which RealPresence Resource Manager system scheduling pages and functions are available to the user role. **Scheduling Level.** This setting determines the level of scheduling available through this role. Possible values are: • **Basic.** Users can schedule conferences using the conference templates defined for them. They cannot access or edit the advanced **Conference Settings**. • **Advanced.** Users can schedule conferences using the conference templates defined for them. They can also access and edit the advanced **Conference Settings**.

4 Click **Save**.

The new user role appears in the RealPresence Resource Manager system.

Edit Permissions for a User Role

You can change permissions for the default 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. As needed, use the **Filter** to customize the **User Roles** list.
3. In the **User Roles** list, select the role of interest and click **Edit**.
4. Edit the **Description** field of the **Edit Role** dialog box and edit permissions for the role.
5. Click Save.

Delete a User Role

You can delete a user role from the RealPresence Resource Manager system, provided no users are currently assigned to it.

To delete a user role

1. Go to **User > User Roles**.
2. As needed, use the **Filter** to customize the **User Roles** list.
3. In the **User Roles** list, select the role of interest and click **Delete**.
4. Click **Yes** to confirm the deletion.

   The user role is deleted from the RealPresence Resource Manager system.

View the Groups and Users Associated with a User Role

To view which groups and users are associated with a specific user role

1. Go to **User > User Roles**.
2. As needed, use the **Filter** to customize the **User Roles** list.
3. In the **User Roles** list, select the role of interest and click **View Associated Groups and Users**.

   The **View Associated Groups and Users** dialog box appears.

Assign Users to Manage an Area(s)

This task is only available if areas have been enabled (multi-tenancy).

In order to perform RealPresence Resource Manager system tasks within an area, the user must be allowed to manage that area. Allowing a user to manage an area means allowing them to perform the duties associated with their role in the areas that they are allowed to manage.

A user can be allowed to manage:

- **Zero areas**. This means that user cannot perform any tasks in any area.
- **One Area.** This means that the user can perform role-based tasks for the area he manages. You must indicate which area you want the user to manage.

- **Multiple areas.** This means the user can perform role-based tasks in each area that he manages. You must indicate which areas you want the user to manage.
- **All areas.** A user can manage all areas if he is assigned a system role or if his role includes the View and/or Modify All areas permission. If the user has this role, you do not need to explicitly allow him to manage an area or areas.

For example, a user with the area scheduler role can belong to the yellow area and allowed to schedule conferences in both the yellow and blue areas if he has permission to manage the blue area as well as the yellow area.

In order to enable a user to manage an area, you must have the administrator role or the area administrator role and manage the area to which you want to allow a user to manage. In short, you need to have permission to manage the area to which you want to allow a user to manage.

To assign a user to manage an area(s)

1. Go to **User > Users**.
2. Enter the name for the user of interest in the **Search Users** field and press **Enter**.

> Searches for a user are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

3. Select the user to assign to an area and choose the **Edit** action.
4. In the **Edit User** dialog, click **Managed Areas**.

   You must have either the administrator role or have the area administrator role and be allowed to manage more than one area in order to perform this action.
5. Select the **Specific Areas** radio button.
6. In the **Available Areas** section, mark the area(s) you want the user to manage and click the arrow icon to move the list to the **Selected Areas** section.

   Conversely, you can mark area(s) in the **Selected Areas** section and click the corresponding arrow to move the marked area(s) to the **Available Areas** section.

   The user will be assigned to manage the areas in the **Selected Areas** section.
7. Click **OK**.

Manage System Guest Book

The Guest Book provides a way to store conference participants that aren’t managed by the RealPresence Resource Manager system.

It includes these topics:

- Guest Book Considerations for Multi-Tenancy on page 312
- User Menu and Guest Book on page 312

- Context-Sensitive Guest Book Actions on page 312
- Add a Guest to the System Guest Book on page 313
- Edit a Guest in the System Guest Book on page 315
- Delete a Guest from the System Guest Book on page 315

Guest Book Considerations for Multi-Tenancy

When areas are enabled for your system, area users can view only those guests who have been assigned to an area that they manage. If a user can manage more than one area, he can view users from all areas that he manages. For more information, see Area Conference Guests on page 432.

User Menu and Guest Book

By default, both system and area schedulers, operator, and administrators have access to the **User Menu** and **Guest Book**.

The **Guest Book** is a local system directory that includes guest participants who were either:

- Explicitly added to the **Guest Book**.
- Saved to the **Guest Book** while being added as conference participants.

They are referred to as static entries because they are not imported through the dynamically updated enterprise directory or included in the system **Global Address Book**. The **Guest Book** is limited to 500 entries. The **Guest Book** has these fields.

Field	Description
Name	The guest’s first and last name.
Email	The guest’s E-mail address. The system validates the E-mail structure only.
Location	The location of the guest’s endpoint system. This is a free-form entry field that the system does not validate.
Number	(Optional) The ISDN phone number for the user. This number is constructed from the Country code + Area/City code + phone number or entered as the modified dial number.
Join Mode	Indicates whether the guest will use an audio endpoint or video endpoint to join conferences.
Dial Options	Indicates whether the guest will dial into conferences or that the system should dial out to the guest.
Dial Type	Indicates whether the guest has an H.323 (IP), SIP (IP), or H.320 (ISDN) endpoint.
Selected Area	This field is available when areas are enabled and the user can manage more than one area.

Context-Sensitive Guest Book Actions

The **Actions** section of the **Guest Book** page may include these context-sensitive actions depending on what is selected.

Actions	Description
Add Guest	Use this command to add a new guest user.
Edit Guest	Use this command to change information for a guest user.
Delete Guest	Use this command to delete a guest from the **Guest Book**. Deleting a guest is a permanent operation.

Add a Guest to the System Guest Book

To add a guest to the system Guest Book

1. Go to **User > Guest Book** and click **Add Guest**.
2. Configure the **Guest Information** section of the **Add New Guest** dialog box.

Field	Description
First Name	The guest’s first name.
Last Name	The guest’s last name.
Email	The guest’s E-mail address. The system only validates the structure of the E-mail address.
Location	The location of the guest’s endpoint system. This is a free-form field that the system does not validate.
Dial Type	Specify the protocol that the guest’s endpoint supports: H.323 (IP), SIP (IP), or H.320 (ISDN). This selection will determine what other sections of the **Add New Guest** dialog box you will need to complete.
Join Mode	Specify whether the guest’s endpoint is an audio or video endpoint. **Note** A guest may have multiple endpoints. Create a separate **Guest Book** entry for each endpoint.
Dial Options	Specify whether the guest will dial into conferences, or require that the system dial out to the guest. **Note** To support both options, create a separate **Guest Book** entry for each.
Assigned Area	This field is available when areas are enabled and the user can manage more than one area.

3 If the guest has an H.323 (IP) endpoint, configure these settings:

Field	Description
Number and Number Type	The specific dial string for the guest, and the format of the number that the MCU must resolve to contact the guest. This may be an IP address, E.164 address, H.323, or Annex-O. For Annex-O dialing, in the **Number** field enter the `H.323.alias@IP`, for example: • `1001@11.12.13.14` • `1001@domain.com` • `username@domain.com` • `username@11.12.13.14` **Notes** • Polycom endpoints must register with a gatekeeper before they will attempt an Annex-O call. • You can enter a dial string for another MCU as a guest. If so, you may need to specify the conference ID in the **Extension** field also.
Extension	Use this field to connect the conference to another conference on another MCU. In this field, specify the conference ID or passcode for the conference on the other MCU.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

4 If the guest has a SIP (IP) endpoint, configure these settings:

Field	Description
Sip URI	The SPI URI the MCU must resolve to contact the guest.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system is registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

5 If the guest has an H.320 (ISDN) endpoint, configure these settings:

Field	Description
Use Modified Dial Number	Select this option first (as needed) as it will determine the other fields you must configure.
Country	(Not available when **Use Modified Dial Number** is selected.) The country to which the system will dial out to the guest. Click **Select** to view a list of country codes.
Area/City Code	(Not available when **Use Modified Dial Number** is selected.) The area code to which the system will dial out to the guest.

Field	Description
Number	The participant's phone number.
Extension	Cannot be configured.
MCU Service	Choose from the list of MCU services defined on the MCUs with which the RealPresence Resource Manager system has registered. Leave this at **Any Available Service** unless you have specific knowledge of MCU services.

6 Click **OK**.

Edit a Guest in the System Guest Book

To edit a guest in the system Guest Book

1 Go to **User > Guest Book** and select the guest of interest.

2 Click **Edit Guest**.

3 Change the **Guest Information** section and endpoint information sections of the **Add New Guest** dialog box, as needed. For more information about these fields, see Add a Guest to the System Guest Book on page 313.

4 Click **OK**.

Delete a Guest from the System Guest Book

To delete a guest from the system Guest Book

1 Go to **User > Guest Book** and select the guest of interest.

2 Click **Delete Guest**.

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

Manage Favorites

The RealPresence Resource Manager system allows users with the **operator role** or **area operator role** to create one or more **Favorites** list, which they can use to quickly select participants to participate in conferences.

The operations associated with managing favorites include:

- Add a Favorites List on page 316
- Edit a Favorites List on page 316
- Delete a Favorites List on page 317

In the RealPresence Resource Manager system, only users with the operator or area operator roles with **Monitoring** permissions can view, add, edit, delete, or use **Favorites** lists and these **Favorites** lists cannot be shared with other operators.

Add a Favorites List

To add a Favorites list

1 Go to **User > Favorites**.

2 On the **Favorites** page, click **Add**.

3 Complete the **Favorites List Name** and **Description** fields of the **Add Favorites List** dialog box.

> The **Favorites List Name** must be unique within the system.

4 In the **Search Available Members** field enter all or part of the person's last name or first name and click **Search**.

The system searches the **Users** list (local and domain) for users who are associated with endpoints and who meet your search criteria. The results appear in the **Search Results** column.

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

5 Select the user(s) of interest from the list and move them to the **Favorite List Members** column.

6 Repeat step In the Search Available Members field enter all or part of the person's last name or first name and click Search. and Select the user(s) of interest from the list and move them to the Favorite List Members column. until you've added the users of interest to your **Favorites** list and then click **OK**.

The new list appears in the **Favorites** page.

Edit a Favorites List

To edit a Favorites list

1 Go to **User > Favorites**.

2 On the **Favorites** page, select the **Favorites** list of interest and click **Edit**.

3 In the **Edit Favorites List** dialog box, edit the **Favorites List Name** and **Description** fields as needed.

4 Remove or add users to the **Favorite List Members** column as needed and then click **OK**.

Delete a Favorites List

To delete a Favorites list

1. Go to **User > Favorites**.
2. On the **Favorites** page, select the **Favorites** list of interest and click **Delete**.
3. Click **Yes** to confirm the deletion.

   The list is deleted from the RealPresence Resource Manager system.

Managing Meeting Rooms

This chapter describes how to set up rooms in the Polycom® RealPresence® Resource Manager system. It includes these topics:

Local and Enterprise Meeting Rooms

The RealPresence Resource Manager system allows a user assigned the default **Administrator** role or the **Area Administrator** role to manage local and enterprise meeting rooms and the endpoints associated with those meeting rooms.

Most often a system is integrated with an enterprise directory to which rooms have been added. However, the system also allows you to add local rooms (that is, rooms added manually to the system) and associate them with endpoints.

If you want to dynamically manage the endpoint associated with a room, you must also associate each room in the system with a machine account. The machine account allows the room's endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user's account. After you add a room, you can create the machine account and associate the room with the machine account. For more information, see Change Database Passwords on page 333.

View the Rooms List

To view the Rooms list

» Go to **User> Rooms**.

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

Column	Description
Room Name	The unique and required name of the room.
Description	The optional description of the room.
Site	The location of the room as identified in the site topology. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Associated Endpoints	The primary endpoint associated with this room. A set of ellipses (...) indicates the room has more than one associated endpoint.
Selected Area	The area to which this room is assigned. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.

Add a Local Room

When you add a local room to your system, you specify room settings and associate one or more endpoints with the room.

Note for Dynamically Managed Endpoints Associated with Rooms

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room's endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user's account.

After you add a room, you can create the machine account and associate the room with the machine account. For more information, see Change Database Passwords on page 333.

To add a local room

1 Go to **User > Rooms**.

2 On the **Rooms** page, click **Add**.

The **Add New Room** dialog box appears.

3 If you are logged into a domain other than the Local domain, click **Manually Define**.

4 Complete the **General Info** and **Associated Endpoints** sections of the **Add New Room** dialog box. The following table shows the room information in the RealPresence Resource Manager system records.

Field	Description
General Info	
Room Name	The name of the room, which appears in the address book for associated endpoints.
Description	(Optional) A useful description (ASCII only) of the room.
Site	The site in which the room is located. **Note** • Rooms and the endpoint associated with them must be assigned to the same site. • When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Email	(Optional) The E-mail address of the room administrator.
Assign Area	Select an area to which to assign this room. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.
Associated Endpoints	
Available Endpoints	The list of unassigned endpoints that are managed by the RealPresence Resource Manager system.
Selected Endpoints	The list of endpoints assigned to the room. The endpoint at the top of the list is the primary endpoint. You can change the order of endpoint priority by selecting a endpoint and clicking Move Up or **Move Down**.

5 In the **SIP Dial String Reservations** section, select the user's **Device Type** and enter the appropriate dial string for **SIP URI**, then click **Apply**.

The dial strings appear in the list below.

By default, the same SIP URI is used for all endpoints that belong to the same user. If the user has multiple endpoints and you want a different SIP URI for each device type, enter the dial strings for one endpoint type at a time and click **Apply** each time.

6 In the **H323 Dial String Reservations** section, select the user's **Device Type** and enter the appropriate dial string for **E164** and **H323 ID**, then click **Apply**.

The dial strings appear in the list below.

If the user has multiple endpoints, enter the dial strings for one endpoint type at a time and click **Apply** each time.

7 Click **OK**.

The room is added to the system. Note that the system does not distinguish between enterprise rooms and local rooms once they've been added to the system.

Add an Enterprise Room

If your system is integrated with an enterprise directory, you can add a room from the enterprise directory to the system.

Note for Dynamically Managed Endpoints Associated with Rooms

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room's endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user's account.

After you add a room, you can create the machine account and associate the room with the machine account. For more information, see Change Database Passwords on page 333.

To add an enterprise room

1 Go to **User > Rooms**.

2 On the **Rooms** list, click **Add Room**.

The **Add New Room** dialog box appears.

3 To find a room in the enterprise directory:

a In the **Search Value** field, type in the first few characters of the room name.

The system does a prefix search of the appropriate fields.

b Click **Search**.

A list of the enterprise users and rooms that meet the search criteria appears. If the search found more than 500 matching entries, only the first 500 are displayed.

c Select the room of interest and click **Define Details**.

4 Complete the **General Info**, **Associated Devices**, and **Dial String Reservations** sections of the **Add New Room** dialog box. For information on these fields, see Add a Local Room on page 319.

5 Click **OK**.

The room is added to the system. Note that the system does not distinguish between enterprise rooms and local rooms once they've been added to the system.

Edit a Room

To edit a room

1 Go to **User > Rooms**.

2 In the **Rooms** list, select the room of interest and click **Edit**.

3 Edit the **General Info**, **Associated Devices**, **SIP Dial String Reservations**, and **H323 Dial String Reservations** sections of the **Edit Room** dialog box. For information on these fields, see Add a Local Room on page 319.

4 Click **OK**.

Note for Dynamically Managed Endpoints Associated with Rooms

If you want to dynamically manage the endpoint associated with a room, you must also associate the room with a machine account. The machine account allows the room's endpoint to connect and authenticate with the system for directory and dynamic management purposes without using the endpoint user's account.

After you add a room, you can create the machine account and associate the room with the machine account. For more information, see Change Database Passwords on page 333.

Delete a Room

To delete a room

1 Go to **User > Rooms**.

2 In the **Rooms** list, select the room of interest and click **Delete**.

3 In the **Delete Room** dialog box, click **Yes**.

The room is deleted from the RealPresence Resource Manager system.

System Configuration

This section provides an introduction to the Polycom® RealPresence® Resource Manager systemconfiguration. It includes:

Securing the System

This chapter describes the Polycom® RealPresence® Resource Manager system management and security tasks. It includes these topics:

Configure Security Settings

You can configure security settings for your system that allow you to maintain higher security levels when necessary. For example, you can disable Linux console access or disallow presence connections.

To configure security settings

1 Navigate to **Admin > Management and Security** and select **Security Options**.

2 You can uncheck the following options to ensure higher security levels:

➢ **Allow XMPP (presence connections)**

XMPP connections are not encrypted, you can disable these.

- **Allow ICMP (ping) responses**

  You can choose to disallow the RealPresence Resource Manager to respond to ping messages.

- **Respond to ICMP (ping) requests with Destination Unreachable message**

  If you choose to allow the server to respond to ping requests, you can configure a Destination Unreachable message.

- **Allow troubleshooting traces**

  Troubleshooting traces are not encrypted, you can disable these.

- **Allow scheduling confirmation emails**

  Scheduling confirmation emails cannot be encrypted. You can disable these.

- **Allow audio-only conferences**

  Audio-only calls prevent the participants from visually identifying the other participants. You can disable these.

- **Allow non-LDAP directory protocols**

  Non-LDAP directory protocols are not secure, you can disable these.

- **Allow non-dynamically managed endpoints and point-to-point scheduling (unsecure dialout)**

  When endpoints are not dynamically managed, dialing out to them is not secure.

- **Allow remote alert emails**

  Remote alert emails can be disabled.

- **Allow Linux console access**

  You can disable Linux console access to the RealPresence Resource Manager server. This setting disables console access for all users.

3 Configure the settings you want and click **Update** when finished.

Update the System Software

To update a RealPresence Resource Manager system with a new software version, complete the following tasks:

1. Download the software upgrade file.
2. Obtain an upgrade key code.
3. Save a backup of the RealPresence Resource Manager system databases.
4. Navigate to **Security > Server Software Upgrade**.

   Browse to select the software upgrade file you downloaded.

5 Click Upgrade.

A warning dialog box displays warning you NOT to close the browser. DO NOT log out of the RealPresence Resource Manager system or close the browser during the upgrade. Doing so will cancel the upgrade process.

6 When the upgrade files are completely unpacked, the warning dialog box disappears. You can now logoff or close the browser window. The upgrade process continues.

At any time during the upgrade, navigate to the following URL to view status:

http://<*REALPRESENCERESOURCEMANAGER_IP*>:8989/upgrading.html

7 Verify the upgrade.

For more information on performing each of these tasks, see the *Polycom RealPresence Resource Manager System Upgrade Guide*.

Change the System User Interface Timeout and Number of Sessions

To change the system user interface timeout and number of sessions

1 Go to **Admin > Management and Security Settings > Session Management**.

2 On the **Session Management** page, configure these settings as needed.

Field	Description
Allow Linux console access	This option allows users to use SSH to access the Linux console of the RealPresence Resource Manager system.
Resource Manager user interface timeout (minutes)	By default, the RealPresence Resource Manager system user interface times out after 10 minutes of inactivity. Use this procedure to change the timeout value for the user interface inactivity timer. Possible value is 5 to 60 minutes.
Maximum number of sessions per user	The number of simultaneous login sessions per user ID. By default, the maximum number of sessions per user ID is 5. Possible value is 1 to 10 sessions.
Maximum number of sessions per system	The number of simultaneous login sessions by all users. By default, the maximum number of sessions by all users is 50. Possible value is 2 to 50 sessions. This setting is available only when RealPresence Resource Manager is in maximum security mode. **Note** If this limit is reached, but none of the logged-in users is an Administrator, the first Administrator user to arrive is granted access, and the system terminates the non-Administrator session that’s been idle the longest.

Field	Description
Associate non-local Resource Manager users with basic scheduler role by default	You can associate all enterprise directory users with the basic scheduler role.
Message to display to be displayed to unauthorized users	You can choose to display a message to unauthorized users, see Change the Message for Enterprise Users without a Role on page 327

3 Click Update.

Give Enterprise Users Default Scheduler Role

By default when local users are added to the RealPresence Resource Manager system, they are assigned the **Scheduler** role. By default, when you integrate a RealPresence Resource Manager system to an Active Directory, enterprise users are not assigned a role. In this case, you must either assign each enterprise user a role, or you can use this procedure to give enterprise users the **Scheduler** role by default.

To give enterprise users default Scheduler role for a RealPresence Resource Manager system

1 Go to **Admin > Management and Security Settings > Session Management**.

2 Mark the **Associate non-local Resource Manager users with basic scheduler role by default** check box.

3 Click Update.

Change the Message for Enterprise Users without a Role

To change the message enterprise users without a role see when they try to log into a RealPresence Resource Manager system

1 Go to **Admin > Management and Security Settings > Session Management**.

2 Edit the **Message to be displayed to unauthorized users**.

For example, enter a message such as “Your username and password are valid, but you have no permissions on this system. Contact your IT department for more information.”

3 Click **Update**.

Control Remote Connections to the System

By default, users can access the RealPresence Resource Manager system through the Linux console. You can disable this ability.

To disallow Linux console access

1 Go to **Admin > Management and Security Settings > Session Management**.

2 Clear the **Allow Linux console access** option.

3 Click **Update**.

Edit Log In Banners

The Banner Configuration page allows users assigned the Administrator role to customize the long and short login banners.

A log in banner is the message that appears when users attempt to access the system. Users must acknowledge the message before they can log in. By default, the long banner field on the Banner Configuration page displays the required Standard Mandatory Notice and Consent Provision for systems operating in a maximum security environment. The short banner field displays a shortened version of this same notice.

The long banner is used for the RealPresence Resource Manager system log in banner. It is also provisioned to HDX systems and RealPresence Group systems that the RealPresence Resource Manager system dynamically manages. The short banner is provisioned if the long banner length exceeds the available display area for the endpoint.

The RealPresence Resource Manager system provides several sample long banners. You can use these banners as is or edit them to create a custom long banner. The RealPresence Resource Manager system provides a single short banner, which you can also customize. If you customize the banners, remember that the long banner message may contain up to 5000 characters. The short banner message may contain up to 1315 characters.

To edit the login banners

1 Go to **Admin > Management and Security Settings > Banner Configuration**.

2 To use one of the existing sample long banners:

a From the **Message** drop-down menu, select the sample banner that most suits your needs.

b Edit the banner as needed. If you edit one of the existing banners, the **Message** menu selection changes to **Custom**.

3 Click **Update**.

Automatic Registration Synchronization

You can configure the RealPresence Resource Manager system to send registration server addressing information for the global directory server (GDS) when the endpoint is registered to the RealPresence Resource Manager system.

> For the RealPresence Resource Manager system, the GDS is the same as the global address book (GAB).

This automatic registration synchronization service only works for endpoints that register with the GDS or are manually added to the RealPresence Resource Manager system after the **Automatic Registration Synchronization** setting is enabled.

So if the **Automatic Registration Synchronization** setting is enabled and an endpoint registers with the GDS, the GDS addressing information is sent to the endpoint. If the **Automatic Registration Synchronization** setting is enabled and an endpoint is added manually to the RealPresence Resource Manager system, the GDS addressing information is sent to the endpoint.

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

- **Automatic Registration Synchronization** works only for endpoints that register with the Global Directory Server after the setting is enabled; it does not automatically register pre-existing endpoints.
- The RealPresence Resource Manager system only supports Automatic Registration Synchronization for Polycom and selected third-party endpoints operating in standard mode. For supported endpoint types, including third-party endpoint types, see Supported Endpoint Types on page 109.

To enable Automatic Registration Synchronization of endpoints

1 Go to **Endpoint > Endpoint Management Settings**.

2 In the **Automatic Registration Synchronization** section of the **Endpoint Management Settings** page, select **Synchronize endpoint registration** and click **Update**.

After you have changed this setting, all endpoints you add are automatically provisioned.

Set Common Passwords for Endpoints

The **Common Password** feature allows you to manage endpoints that have the same global administrative password. However, it cannot reset the administrative password on endpoints.

If you use the **Common Password** feature, access to password-protected data within endpoints is granted if the specified common password matches the endpoints’ **Administrator Password**.

To set common passwords for endpoints

1 Go to **Endpoint > Endpoint Management Settings**.

2 In the **Common Password** section of the **Endpoint Management Settings** page, select **Use a Common Password**.

3 Enter the common **User Name** and the common password in the **Password** and **Verify Password** fields and click **Update**.

Leave these 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.

To set default passwords for LifeSize endpoints

1. Go to **Endpoint > Endpoint Management Settings**.
2. In the **Common Password** section of the **Default Passwords for LifeSize Endpoint Management** section, select **Use Default Passwords**.
3. Enter the default password you want to use for LifeSize endpoints in the **Password for user (auto)** field and then re-type the password in the **Verify Password** field.
4. Enter the default password you want to use for the web UI user in the **Password for Web UI User** field and then re-type the password in the **Verify Password** field.
5. Click **Update**.

Disable Common Password for Endpoints

To disable common passwords for endpoints

1. Go to **Endpoint > Endpoint Management Settings**.
2. In the **Common Password** section of the **Endpoint Management Settings** page, clear **Use a Common Password** and click **Update**.
3. For LifeSize endpoints, clear the **Use Default Password** check box and click **Update**.

   The common password feature is disabled. However, the values for the common password feature are retained in the database, so you can easily re-enabled it.

Set Local Account Lockout and Timeout

To set local account lockout and timeout

1. Go to **Admin > Management and Security Settings > Local User Account Configuration**.
2. On the **Local User Account Configuration** page, configure these settings as needed.

Field	Description
Account Lockout	
Failed login threshold	Specify how many consecutive login failures cause the system to lock an account. Possible value is 2 to 10.
Failed login window (hours)	Specify the time span within which the consecutive failures must occur in order to lock the account. Possible value is 1 to 24.
Customized user account lockout duration (minutes)	Specify how long the user’s account remains locked. Possible value is 1 to 480.

Field	Description
Account Inactivity	
Customize account inactivity threshold (days)	Specify the inactivity threshold that triggers disabling of inactive accounts. Possible value is 30 to 180.

3 Click **Update**.

Set Local Password Requirements

The **Local Password Requirements** page allows users assigned the **Administrator** role to change, but not disable password, security requirements by specifying password age, length, and complexity.

To set local password requirements

1 Go to **Admin > Management and Security Settings > Local Password Requirements**.

2 On the **Local Password Requirements** page, configure these settings as needed.

Field	Description
Password Management	
Minimum length (characters)	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Reject previous passwords	Specify how many of the user’s previous passwords the system remembers and won’t permit to be reused. Possible value is 8 to 16.
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.

Field	Description
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

Field	Description
Password Management	
Minimum length (characters)	Specify the number of characters a password must contain. Possible value is 8 to 18.
Minimum changed characters	Specify the number of characters that must be different from the previous password. Possible value is 1 to 4.
Minimum password age (days)	Specify how frequently a password can be changed. Possible value is 1 to 30.
Maximum password age (days)	Specify at what age a password expires. Possible value is 30 to 180.
Password warning interval (days)	Specify when users start to see a warning about their password expiration. Possible value is 1 to 7.
Reject previous passwords	Specify how many of the user’s previous passwords the system remembers and won’t permit to be reused. Possible value is 8 to 16.
Password Complexity	
Lowercase letters	Specify the number of lowercase letters (a-z) that a password must contain. Possible value is 1 or 2.
Uppercase letters	Specify the number of uppercase letters (A-Z) that a password must contain. Possible value is 1 or 2.
Numbers	Specify the number of digit characters (0-9) that a password must contain. Possible value is 1 or 2.
Special characters	Specify the number of non-alphanumeric keyboard characters that a password must contain. Possible value is 1 or 2.
Maximum consecutive repeated characters	Specify how many sequential characters may be the same. Possible value is 1 to 4.

3 Click **Update**.

Configuring a Whitelist

You can configure a whitelist of IP addresses that are allowed to access the RealPresence Resource Manager system’s web interface or SNMP information.

When you enable the whitelist feature, only IP addresses included on the whitelist will be allowed to access the RealPresence Resource Manager system’s web interface or SNMP information

To configure a whitelist of IP addresses

1. Navigate to **Admin > Management and Security > Whitelist** to view the **Whitelist** screen.
2. In the Whitelist screen, mark the **Enable Whitelist** check box.
3. Click **Actions > Add**.
4. In the **Add Whitelist** dialog box, specify the IP address(s) to be included.

   You can specify IP addresses individually or as a range. If IPv6 is enabled, you can enter either an IPv4 address or range or an IPv6 address or range.
5. Click **Update** to save the IP address to the whitelist.

   Repeat these steps to continue adding IP addresses or ranges of IP addresses until finished.
6. Click **Update** on the main page to save your whitelist.

To disable whitelists

If you have enabled a white list and want to disable it, unmark the **Enable Whitelist** check box.

Change Database Passwords

The RealPresence Resource Manager system uses five user names to access its database. You can change the passwords for those user names to comply with any requirements you may have to change passwords on a regular basis.

You also use the user listed as **PlcmDbo** if you should need to reformat your internal database. For more information, see Reformat the Existing Database on page 454.

The system will restart after you change these passwords. Make sure that you use this function when no conferences are active or scheduled.

To change internal database passwords

1. Go to **Admin > Management and Security Settings > Database Security**.
2. Select the database user whose password you want to change.
3. Click **Change Password**.
4. In the Change Database User Password dialog, enter the new password in the **New Password** and **Confirm New Password** fields.

   If you want the system to generate a password, click **Create Password**. Be sure to write down the password that displays.
5. Click **OK**.

6 Click **Apply Password Changes**.

The system resets the passwords and restarts. It may take the RealPresence Resource Manager system up to 10 minutes to shut down and then restart all server processes.

Editing SNMP Settings

Please see Polycom RealPresence Resource Manager System SNMP on page 468 for more information about managing SNMP settings.

Setting Up the RealPresence Resource Manager System

This chapter describes how to update the Polycom® RealPresence® Resource Manager system configuration settings, many of which were entered during **First Time Setup**. It includes these topics:

Edit the System Network Settings

Edit the system **Network** settings to change the basic network information for the RealPresence Resource Manager system.

Note

If you are using security certificates, you must request and install a new certificate (or certificate chain) if you change the following network settings:

- If you switch to support from multiple IP protocols to single such as from IPv4 to IPv4 and IPv6 or vice versa, you will need a new certificate.
- If you change the system name, you will need a new certificate.
- If you change the DNS domain name, you will need a new certificate.

To edit the RealPresence Resource Manager system network settings

1 Go to **Admin > Server Settings > Network**.

2 Configure these settings on the **Network** page, as necessary.

Field	Description
Supported Network Types	Choose the type of network on which the RealPresence Resource Manager resides: • IPv4 only • IPv4 and IPv6 • IPv6 only
System Name	The NetBIOS name (ASCII only) of the RealPresence Resource Manager system server. Must be between 6 and 16 characters long; dashes and underscores are valid characters.
DSCP Marker	Allows the administrator to configure the Quality of Service level of the RealPresence Resource Manager. Set the level between 0 - 63. The higher the number the higher the Qualify of Service level.
IPv4 Address	The static IPv4 address for the RealPresence Resource Manager system.
IPv4 Subnet Mask	The network subnet mask for the RealPresence Resource Manager system IP address.
IPv4 Default Gateway	The static IP address of the RealPresence Resource Manager system gateway.
DNS Domain	The DNS domain name suffix for the network in which the domain name server and RealPresence Resource Manager system server reside. For example polycom.com, not the fully qualified path of <*hostname*>`.polycom.com`. **Note** If instead of entering a single domain controller, you enter an FQDN that maps to multiple servers, be sure that all of the mapped servers are directory domain controllers with global catalogs.
Preferred DNS Server	The IP address of the preferred domain name server for the network.
Alternate DNS Server	The IP address of the alternate domain name server for the network.

3 Click **Update**.

If you change the IP address, the system prompts you to restart the RealPresence Resource Manager system. We also recommend that you restart the system if you change the subnet mask.

4 As required, restart the system.

Edit the System Time Settings

Edit the **System Time** server settings to change the RealPresence Resource Manager system server time or to synchronize the server with an external NTP server.

To edit the RealPresence Resource Manager system time settings

1 Go to **Admin > Server Settings > System Time**.

2 Configure these settings on the **System Time** page, as necessary.

Field	Description
System Time Zone	The time zone in which the Resource Manager system server resides.
Use Current Time	Select this option to input the current date and time.
Use External NTP Server Time Synchronization	Select this option to synchronize the Resource Manager system date and time with an external NTP server.
IP address or DNS resolved name	The IP address or fully qualified domain name (ASCII only) of the NTP server. If needed, enter multiple servers separated by a space.

Note

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**.

3 Click **Update**.

Integrate with Microsoft Exchange Server for Calendaring Management

The RealPresence Resource Manager system can be used to provision Polycom Conferencing for Microsoft Outlook, which is reservationless conferencing. When you use Polycom Conferencing for Microsoft Outlook:

- Video bridge, network resources, and video endpoints are not reserved at the scheduled time.
- A Polycom RMX or DMA system is required to locate available bridge resources when the meeting begins.
- Calendars for the endpoints are stored and maintained by Microsoft Exchange and the endpoints have their own Outlook calendar.

Polycom Conferencing for Outlook, which requires the Polycom Conferencing Add-in, allows:

- Conference organizers to:
  - ➢ Use Microsoft Outlook and its usual meeting request workflow to schedule video- and audio-enabled meetings.

  - ➢ Include recording and streaming into the conference, when required.

- Meeting participants to:
  - ➢ Track their video- and audio-enabled meetings on the same calendar that they track their other meetings.
  - ➢ Click a link in an E-mail meeting request to join conferences on their associated video or audio endpoint system.
- Endpoints to have their own unique credentials and mailbox separate from the endpoint user, so that endpoints can display their own calendars. This is especially important for room endpoints.

To provision endpoints with the information required to support Polycom Conferencing for Outlook, you must complete the following tasks (after your sites are set up):

1. Associate Sites with Microsoft Exchange Servers on page 338.
2. Assign Calendaring Settings to Provisioning Profiles on page 338.
3. Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints on page 339.

Associate Sites with Microsoft Exchange Servers

By default, the RealPresence Resource Manager system is set up to automatically discover the Exchange server for the domain in which a site is located. However, if you wish to associate sites with an Exchange server using its IP address or DNS name, follow this procedure.

To associate sites with Microsoft Exchange servers by IP address or DNS name

1. Go to **Admin > Server Settings > Calendaring Management**.
2. In the **Manage Calendaring** dialog box, click **Calendared Sites**.

   The **Specify Calendaring Exchange Servers** page appears listing the sites defined on the Resource Manager system.

   When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
3. Select the check box for each of the sites you need to associate with a single Exchange server and then click **Specify Exchange Server**.
4. In the **Add Exchange Server** dialog box, enter the **Exchange Server Address** or DNS and click **Save**.

   The sites appear in the calendared sites list below.
5. Repeat steps 3 and 4 for each Exchange server for which you need to associate sites.

Assign Calendaring Settings to Provisioning Profiles

Calendaring settings are included as part of provisioning profiles.

To assign calendaring settings to provisioning profiles

1 Go to **Admin > Server Settings > Calendaring Management**.

2 In the **Manage Calendaring** dialog box, click **Group Information**.

The **Group Information** page appears listing the provisioning profiles defined on the Resource Manager system.

3 Select the check box for each of the provisioning profiles to which you need to assign the same calendaring settings and then click **Specify Options**.

4 In the **Manage Calendaring** dialog box, configure these options.

Fields	Description
Meeting Reminder Time	Specifies the number of minutes before the meeting an endpoint system provisioned for Polycom Conferencing for Outlook will display a reminder.
Enable Alert Tone	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will play a sound along with the meeting reminder. In this case, the endpoint will only play a sound when the system is not in a call.
Display Private Meetings	When enabled, specifies that an endpoint system provisioned for Polycom Conferencing for Outlook will display details about meetings marked private.

5 Click **Save**.

The profiles appear in the calendared profiles list below.

6 Repeat steps 3 through 5 for each set of profiles to which you need to assign calendaring settings.

Provision the Exchange Mailbox for Calendaring Service-enabled Endpoints

To use Polycom Conferencing for Outlook (PCO), a Polycom endpoint system must have a mailbox on the assigned Exchange server, and the Exchange server must authenticate the endpoint before it can access its mailbox.

To use the Resource Manager system to automatically provision a Polycom endpoint system, the endpoint system must use the same credentials (username and password) to access both the Exchange server and the Resource Manager system. Only then can the Resource Manager system automatically provision a calendaring service-enabled endpoint system.

To provision the Exchange Mailbox for calendaring service-enabled endpoints

1 Go to **Admin > Server Settings > Calendaring Management**.

2 In the **Manage Calendaring** dialog box, click **Mailbox**.

3 In the **Polycom Conferencing for Outlook** page, enable **Provision Mailbox** and click **OK**.

For Exchange credentials, each endpoint system will be provisioned with the same credentials it used to access the Resource Manager system.

For its mailbox, each endpoint system will be provisioned with the mailbox configured for it in Active Directory. This mailbox must be pre-configured for the endpoint system on the Exchange server.

View Current System Licensing

To view current Resource Manager system licensing

» Go to **Admin > Server Settings > Licenses**.

The **Licenses** page displays the following information.

Field	Description
Software Version	
Serial Number	
Supported Versions	
Server Type	
License Status	
Set Duration	
Feature License	
Reclaim Inactive RealPresence Software Client Licenses	

System Licensing

The device management capacity for a RealPresence Resource Manager system with the scales from 500 to 50,000 devices. The minimum capacity of a RealPresence Resource Manager system is of 500 client access licenses. Additional licensing is offered in 100, 500, and 1000 license pack sizes.

Your system comes with a Default Trial license file that is valid for 60 days after activating your system. The Default Trial License also enables the optional Polycom DMA system integration, multi-tenancy, and Service Provider API capabilities for 60 days.

With your system order, you will receive one License Certificate. You must activate the License Certificate to receive a license file, which you then upload to the RealPresence Resource Manager system. When you update this license file, it overwrites the Default License File.

When applied to the system, an expansion license pack augments the device license count. For example, applying a 1000-device expansion license pack to a baseline RealPresence Resource Manager system will yield a total license count of 1500 concurrent licenses.

Device licenses are consumed based on a 1:1 basis for any managed device (endpoints, MCU, 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.

RealPresence Immersive Studio systems consume three device licenses, one for each codec.

Note

Device licenses are consumed by managed devices, not by users. You may add any number of local or enterprise users to the RealPresence Resource Manager system.

The RealPresence Resource Manager system has the following feature licenses:

Field	Description
DMA Integration	Allows you to integrate with a Polycom DMA system as both a call server (gatekeeper) and conference manager
Multi-Tenant	Allows you to use the areas feature to partition collections of resources.
Management of Endpoints and Services	Determines the number of devices you can manage.
Service Provider API	Allows you to access RealPresence Resource Manager functionality via the API
Redundant system licenses (primary and redundant licenses)	Allows you to set up redundant systems.

Licensing for RealPresence software clients is included with the RealPresence Resource Manager system. RealPresence software clients include Polycom CMA Desktop and RealPresence Mobile clients.

When either client is provisioned by the RealPresence Resource Manager system, it automatically consumes a license. That license is then reserved for that client. However, you can configure the system to automatically release a RealPresence client license after a set number of days of inactivity.

Licenses consumed by registered hardware devices are never automatically released. To release a license from a registered hardware device, an administrator must manually delete the device from the system.

Add System Licenses

Adding licenses to your RealPresence Resource Manager system is a two step process:

- Request a Software License File on page 342.
- Update the License File on page 342

These processes are described in the following topics.

Request a Software License File

To request a software license file

1. In a separate browser page or tab, log into the RealPresence Resource Manager system server as an administrator.
2. Go to **Admin > Server Settings > Licenses** and record the RealPresence Resource Manager system server serial number:

   ____________________.
3. Go to http://support.polycom.com.
4. In the **Licensing & Product Registration** section, select **Activation/Upgrade**.
5. Log in or Register for an Account.
6. Select **Site & Single Activation/Upgrade**.
7. In the **Site & Single Activation** page, enter the serial number you recorded in step Go to Admin > Server Settings > Licenses and record the RealPresence Resource Manager system server serial number:.
8. Click **Next**.
9. Accept the **EXPORT RESTRICTION** agreement.
10. In the new **Site & Single Activation** page, enter the serial number listed on your License Certificate and enter the license number (shipped with the product) and click **Activate**.

    If retrieving licenses for a redundant system, repeat this step for each server in your configuration. You will need to load both license files onto your primary server, see System Redundancy on page 447.
11. In the **Key Code** field, click **click here to download** to retrieve and save your license files.

When you have a redundant RealPresence Resource Manager system, you'll need a license file for each system in your configuration. Enter each serial number separately.

Update the License File

You can update the license file for your system at any time. After you update a license file, you must logout and re-login to the system to see newly licensed features.

To update the license file

1. Go to **Admin > Server Settings > Licenses**.
2. Click **Update License** to view the **Update License** dialog box.
3. Click **Choose File** to navigate to the license file you received from Polycom.
4. Click **Preview** to preview the license features.

5. On the **Update License** dialog box, click **Update**.
6. You must log out of the system and log back in to view any new licensed features such as multi-tenancy or DMA integration features.

Reclaim Polycom CMA Desktop and RealPresence Mobile Licenses

Polycom RealPresence Desktop, RealPresence Mobile and CMA Desktop clients do not release licenses automatically when they are not in use. You can reclaim software client licenses by setting a reclaim threshold.

To reclaim licenses more quickly, lower the threshold. Set the threshold to zero to stop reclaiming licenses. You can select a threshold time limit of days, hours or minutes.

To set the threshold for reclaiming inactive RealPresence Software Client licenses

1. Go to **Admin > Server Settings > Licenses**.
2. Change the **Threshold** value in the **Reclaim Inactive RealPresence Software Client (Mobile and Desktop) Licenses** section of the **Licenses** page. To reclaim licenses more quickly, lower the threshold. Set the threshold to zero, to stop reclaiming licenses.
3. Click **Update**.

Add or Remove a System Logo

You can add your company's logo to the RealPresence Resource Manager system user interface. To avoid distortion, we recommend adding a logo in GIF, JPG, or PNG format with a size of 300 x 44 pixels.

When Areas Are Enabled

- The system logo added with these steps is viewed only by users with system roles that have permission to view all areas and do not belong to an area.
- To customize a logo for an area, you must use the Admin > Area Logos option, see Customize the Area Logos (system and CMA Desktop) for the Area.

To add a custom logo to the RealPresence Resource Manager system user interface

1. Go to **Admin > Server Settings > System Logos**.
2. In the **Current Logo** section of the **System Logos** page, click **Upload...**
3. In the **Select file** dialog box, browse to the logo image and select the file.
4. Click **Open**.

To remove a system logo from the RealPresence Resource Manager system user interface

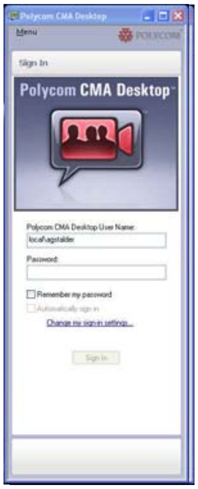
1. Go to **Admin > Server Settings > System Logos**.

2 In the **Current Server Logo** section of the **System Logos** page, click **Remove**.

Add or Remove a Polycom CMA Desktop Custom Logo

You can add your company logo to the Polycom CMA Desktop user interface. This logo will be displayed on the application user interface before the user logs in. The following illustration shows the default Polycom CMA Desktop user interface and a customized Polycom CMA Desktop user interface.

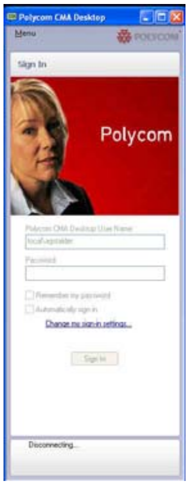
Default Polycom CMA Desktop



Polycom CMA Desktop User Name: local\agstalder

Password:

Branded Polycom CMA Desktop



Polycom CMA Desktop User Name: local\agstalder

Password:

Disconnecting...

To avoid distortion, use a logo in GIF or JPG format with a size of approximately 260x215 pixels.

To add a custom logo to the CMA Desktop user interface

1 Go to **Admin > Server Settings > System Logos**.

2 In the **CMA Desktop Logo** section of the **System Logos** page, click **...** to browse to a logo file to use.

3 In the **Select file** dialog box, browse to the logo image and select the file.

4 Click **Open**.

5 Click **Upload**.

Once a user logs in, is provisioned, and then logs out, the logo will be displayed on the Polycom CMA Desktop user interface.

To remove a custom logo from the CMA Desktop user interface

1 Go to **Admin > Server Settings > System Logos**.

2 In the **Current CMA Desktop Logo** section of the **System Logos** page, click **Restore Default**.

Once a user logs in, is provisioned, and then logs out, the default logo will be displayed on the CMA Desktop user interface.

Edit the System E-mail Account

To edit the RealPresence Resource Manager system e-mail account

1 Go to **Admin > Server Settings > E-mail**.

2 On the **E-mail** page, edit the e-mail account (ASCII only) from which the RealPresence Resource Manager system will send conference notification e-mails or edit the IP address of the mail server from which the Resource Manager system will send conference notification e-mails.

Notes

- Many e-mail servers will block or discard e-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
- Many E-mail servers will block or discard e-mails from un-trusted domains, in which case you may need to change the default RealPresence Resource Manager system E-mail address to one in a trusted domain.

3 Click **Update**.

Managing Security Certificates

Certificates are a security technology that assists networked computers in determining whether to trust each other. Each digital certificate is identified by its public key. The collection of all public keys used in an enterprise to determine trust is known as a Public Key Infrastructure (PKI).

To manage digital certificates, an enterprise must:

- Establish a Public Key Infrastructure using one or more Certificate Authorities (CA). Typically, an enterprise's IT department has a CA but commercial CAs may be used as well.
- Configure each computer that participates in the PKI with a digital certificate that identifies it. The certificate must be signed by one of the CAs in the PKI.
- Configure each computer that participates in the PKI to trust the PKI's Certificate Authorities.
- Ensure that the PKI is used to protect data exchange by configuring each system to use encryption protocols such as Secure Sockets Layer (SSL) and/or Transport Level Security (TLS).

This chapter describes the Polycom® RealPresence® Resource Manager system certificate management tasks. It includes these topics:

- Configuring RealPresence Resource Manager to Use Certificates on page 346
- Configuring Certificate Settings on page 347
- Installing Certificates on page 349
- Configuring OCSP Settings on page 358

Configuring RealPresence Resource Manager to Use Certificates

Before installing any certificates or configuring an Online Certificate Status Protocol (OCSP) responder settings, you must configure how the RealPresence Resource Manager system will use certificates.

These settings specify, for example, whether the RealPresence Resource Manager system is allowed to have a self-signed certificate and the validation options that should be applied to certificates from other systems.

Certificate settings also specify if client systems (endpoints and users who access the RealPresence Resource Manager system user interface) require to present certificates for authentication. Determine the degree in which you want to use certificates within your deployment and configure the settings appropriately.

1 Configuring Certificate Settings on page 347

2 Installing Certificates on page 349.

3 Configuring OCSP Settings on page 358

Configuring Certificate Settings

You can configure how the RealPresence Resource Manager deals with security certificates. How you set up your certificate settings determines the level of security you have for your system.

For example, you can require all clients attempting to access the system to present a certificate. You can also allow the system to trust self-signed certificates. The latter example represents a less secure configurations and is not allowed in maximum security environments.

> Using Self-Signed Certificates
>
> If you install a full PKI chain after you configured the system to trust self-signed certificates, you should delete the self-signed certificates of any system on which the self-signed certificate has been replaced with a CA signed certificate.
>
> Self-signed certificates are not allowed when the system is in maximum security mode.

To configure certificate settings

1 Go to **Admin > Management and Security > Certificate Management**.

2 Click **Certificate Settings**.

3 For **Server Settings**, use the following table as guidance:

Field	Description
Cipher Mode	You can choose from the following cipher modes: Standard Ciphers Weak Ciphers Strong Ciphers (FIPS)
Allow self-signed certificate	You can choose to allow a self-signed certificate on the RealPresence Resource Manager system.
Require client to send certificate	This setting requires all clients (endpoints, peripherals, and users accessing the RealPresence Resource Manager system web interface over an encrypted protocol such as SSL or TLS) to send identity certificates in order to access the system.

4 For **External Client Certificate Settings**, use the following guidance:

Field	Description
Trust self-signed certificate	You can choose to trust self-signed certificates from client systems (endpoints, users accessing the web interface, and peripherals). Use this setting with discretion. Any and all self-signed certificates presented by clients will automatically be installed as trusted peer certificates and will be trusted until they are deleted from RealPresence Resource Manager's trusted certificates list. This setting is intended to be used selectively, for example, during initial deployment of a Polycom solution that will use self-signed certificates going forward. After RealPresence Resource Manager has been running for several hours (or days) and all of the known clients' certificates have been added to the RealPresence Resource Manager's trusted certificates list, the setting should be disabled to prevent network intrusion from unknown clients. Disabling the setting does not mean that self-signed certificates will no longer be trusted. It means that no new self-signed certificates will be automatically added to the RealPresence Resource Manager's trusted certificate list.
Validate date range	Choose if you want to validate the date range. When this is checked, the RealPresence Resource Manager verifies the date range contained in the certificate to ensure validity.
Validate revocation	When this is checked, the RealPresence Resource manager validates the revocation status using the revocation resources (OCSP responder URL or CRL Distribution Point).

5 For **External Server Certificate Settings**, use the following guidance:

Field	Description
Trust self-signed certificate	This option is disabled when the system is in maximum security mode. You can choose to trust self-signed certificates from server systems (DMA systems, MCUS and session border controllers). Use this setting with discretion. Any and all self-signed certificates presented by servers will automatically be installed as trusted peer certificates and will be trusted until they are deleted from RealPresence Resource Manager's trusted certificates list. This setting is intended to be used selectively, for example, during initial deployment of a Polycom solution that will use self-signed certificates going forward. After RealPresence Resource Manager has been running for several hours (or days) and all of the known servers' certificates have been added to the RealPresence Resource Manager's trusted certificates list, the setting should be disabled to prevent network intrusion from unknown servers. Disabling the setting does not mean that self-signed certificates will no longer be trusted. It means that no new self-signed certificates will be automatically added to the RealPresence Resource Manager's trusted certificate list.

Field	Description
Validate hostname	When this is checked, the RealPresence Resource Manager verifies the hostname contained in the certificate to ensure validity.
Validate date range	Choose if you want to validate the date range. When this is checked, the RealPresence Resource Manager verifies the date range contained in the certificate to ensure validity.
Validate revocation	When this is checked, the RealPresence Resource manager validates the revocation status using When this is checked, the RealPresence Resource manager validates the revocation status using the revocation resources (OCSP responder URL or CRL Distribution Point).

6 Click OK.

The next step is to install the required certificates on the RealPresence Resource Manager system.

Installing Certificates

Installing certificates after you have configured your network settings. If you update your network settings (for example, if you change FQDN or change the network protocol IPv4 to IPv6), you must reconfigure certificates for your system,

This section includes the following topics:

- Accepted Certificates on page 349
- Create a Certificate Signing Request on page 351
- Install a Certificate on page 353
- Remove a Certificate from the System on page 354
- Regenerating a Default Certificate on page 355
- Revert to Legacy VVX Certificate on page 356
- View Certificates and Certificate Details on page 357

Accepted Certificates

To support encrypted communications and establish a minimum level of trust, the RealPresence Resource Manager system presents a self-signed digital certificate to its clients. This default certificate will typically not be trusted by clients. Web browsers that connect to the RealPresence Resource Manager system user interface will display a warning regarding the certificate.

Participation in a Public Key Infrastructure requires a RealPresence Resource Manager system to have been configured with at least one root CA certificate, and a digital certificate signed by that CA that identifies the RealPresence Resource Manager system.

However, you will often need additional CA certificates to allow the system to properly validate a received certificate. Work with your network administrator to gather all required certificates needed for use in the environment. Here is a simple checklist:

- RealPresence Resource Manager Identify Certificate - created by the system via the Certificate Signing Request (CSR) procedure described below and signed by a CA within your network infrastructure).
- CA certificate for the CA that signs the RealPresence Resource Manager Identity Certificate
- A root CA certificate - this is the certificate for the root of the CA hierarchy.
- The CA certificates for all intermediate CAs between the root CA and the CA that signs the RealPresence Resource Manager identity certificate.
- The certificate used to validate responses from the OCSP responder (see Revert to Legacy VVX Certificate on page 356).

Certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed in the RealPresence Resource Manager system.

Encoding	Standard / File Type	Description and Installation Method
PEM (Base64-encoded ASCII text)	PKCS #7 standard P7B file	Certificate chain containing: • A signed certificate for the system. • The CA's public certificate. • Sometimes intermediate CA certificates. Upload file or paste into text box.
	CER (single X.509 certificate)	Signed certificate for the system. Upload file or paste into text box.
	Certificate text (can be PKCS#7(P7B) or a single X.509 certificate)	Encoded certificate text copied from CA's E-mail or secure web page. Paste into text box.

Encoding	Standard / File Type	Description and Installation Method
DER (binary format using ASN.1 Abstract Syntax Notation)	PKCS #12 standard PFX file	Certificate chain containing: • A signed certificate for the system. • A private key for the system. • The CA's public certificate. • Sometimes intermediate CA certificates. Upload file. **NOTE** This format does not require a Certificate Signing Request to have been generated by the RealPresence Resource Manager system. **PKCS #12 is not supported when the RealPresence Resource Manager system is in maximum security mode or when Strong Ciphers (FIPS) mode is being used.**
	PKCS #7 standard P7B file	Certificate chain containing: • A signed certificate for the system. • The CA's public certificate. • Sometimes intermediate certificates. Upload file.
	CER (single certificate) file (X.509 standard format)	Digital certificate that uniquely identifies the system within the PKI. Upload file. **Note** The certificate must have issued by a CA using the most recent Certificate Signing Request generated by the RealPresence Resource Manager system.

Create a Certificate Signing Request

The initial RealPresence Resource Manager system configuration permits using the default, self-signed certificate.

Normal operation in a secure mode requires that you install a digital certificate signed by a trusted certificate authority that uniquely identifies the RealPresence Resource Manager system within your public key infrastructure. This can be done by creating a certificate signing request for the RealPresence Resource Manager system and submitting it to a certificate authority to be signed.

> Although it is common for a system to be identified by any number of digital certificates, each signed by a different CA, the RealPresence Resource Manager system currently only supports a single identity certificate.

This procedure describes how to create a certificate signing request (CSR) to submit to a certificate authority.

To create a certificate signing request

1 Go to **Admin > Management and Security > Certificate Management**.

The **Certificate Management** page displays the list of currently available certificates. By default, the system will have one server certificate identified as the **Resource Manager self-signed certificate** and one or more root certificates or certificate chains.

2 Click **Create Certificate Signing Request**.

If you see the warning “This action will overwrite any previously generated or uploaded private key. Do you want to continue?,” do one of the following:

- If you are waiting for a previous request to be signed, click **No**. Because the RealPresence Resource Manager system currently supports only one identity certificate, only the most recent private key is retained. The digital certificate resulting from the most recent CSR is the only certificate that will match the retained private key and is therefore the only identity certificate that can be installed.
- If this is a new certificate signing request, click **Yes** to continue.

3 In the **Certificate Information** dialog box, enter the identifying information for your RealPresence Resource Manager system and click **OK**.

Field	Description
Signature Algorithm	You can select either SHA256 or SHA1.
Country Name	Two-letter (ASCII only) ISO 3166 country code in which the server is located.
State or Province Name	Full state or province name (ASCII only) in which the server is located.
Locality Name	City name (ASCII only) in which the server is located.
Organization Name	Enterprise name (ASCII only) at which the server is located.
Organizational Unit Name	Subdivision (ASCII only) of the enterprise at which the server is located. Optional. Multiple values are permitted, one per line.
Common Name (CN)	The FQDN (fully-qualified domain name) of the system (read-only), as defined in the network settings.
IPv4 Address	The IPv4 address of the system (read-only), as defined in the network settings.
IPv6 Address	When applicable, the IPv6 address (read-only) of the system, as defined in the network settings.
Email Address	E-mail address (ASCII only) for a contact at the enterprise.

A **File Download** dialog box appears.

4 In the **File Download** dialog box, click **Save**.

5 In the **Save As** dialog box, enter a unique name for the file, browse to the location to which to save the file, and click **Save**.

6 Submit the file (or text within the file) as required by your certificate authority.

> Since RealPresence Resource Manager uses this single certificate for both TLS client and TLS server connections, it is important that the certificate template used on the CA enable both "clientAuth" and "serverAuth" use in the "Extended Key Usage" (EKU) field of the certificate. Related bits in the "Key Usage" extension should be set accordingly per RFC 5280 guidance. Work with the administrator of the CA to assure this.

When your certificate authority has processed your request, it sends you a signed digital certificate for your RealPresence Resource Manager system. Some certificate authorities send only the signed digital certificate while others send all of the certificates that form the chain of trust (including intermediate and/or root CA certificates). These certificates may arrive as e-mail text, e-mail attachments, or be available on a secure web page.

Install a Certificate

This procedure describes how to install a certificate or certificate chain provided by a certificate authority. It assumes that you’ve received the certificate or certificate chain in one of the formats accepted by the RealPresence Resource Manager system. See Accepted Certificates on page 349.

> Installing certificates requires a system restart.
>
> When you install a certificate, the change is made to the certificate store immediately, but the system will not recognize or use the new certificate until it restarts and reads the changed certificate store.

To install a signed certificate that identifies the RealPresence Resource Manager system

1 Go to **Admin > Management and Security > Certificate Management** and click **Install Certificates**.

A warning appears stating that changes made to the certificates will require a system restart to take effect.

2 In the **Install Certificates** dialog box, do one of the following:

- If you have a PKCS#12, PFX, P7B, or single certificate file, click **Upload certificate**, enter the password (if any) for the file, and browse to the file or enter the path and file name.
- If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box at the bottom of the dialog box. You can paste multiple PEM certificates one after the other.

3 Click **OK**.

If you are uploading a signed identity certificate for the first time, it will replace the RealPresence Resource Manager system self-signed certificate.

4 Verify that the new signed certificate has replaced the default self-signed certificate:

   a In the list of certificates, select the **Resource Manager certificate** and click **View Certificate Details**.

   b When the **Certificate Details** dialog box appears, verify that the information in the **Issued To** sections matches the FQDN of the RealPresence Resource Manager and the certificate from the certificate authority and that the information in the **Issued By** section matches the expected name of the certificate authority.

   c Click **Close** to close the dialog box.

   Use the same procedure to install other certificates as needed (intermediate CA certificates, root CA certificates, certificate used to validate OCSP responses). You need to have all CA certificates installed that are part of the chain of trust for any client or server identity certificate that the system may be presented and be required to validate on any of its external connections. Work with your network administrator to determine this list.

Note

The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

Remove a Certificate from the System

You can delete certificates from the system, but the RealPresence Resource Manager system prevents you from deleting any certificate that breaks the identity certificate's chain of trust. To delete these certificates, new CA certificates must be installed and the identity certificate must be replaced.

There are two kinds of certificate removal:

- Removing the certificate of a Trusted Root CA so that the system no longer trusts certificates signed by that certificate authority.
- Removing the signed certificate currently in use as the certificate so that the system reverts to using the default self-signed certificate.

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

Both procedures are described below.

Caution

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

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

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

To remove a Trusted Root CA's certificate

1. Navigate to **Admin > Management and Security > Certificate Management**.
2. In the certificates list, select the certificate you want to delete.
3. In the **Actions** list, select **View Certificate Details** and confirm that you've selected the correct certificate. Then click **OK.**
4. In the **Actions** list, select **Delete Certificate**.
5. When asked to confirm, click **Yes**.

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

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

1. Navigate to **Admin > Management and Security > Certificate Management**.
2. In the certificates list, select the certificate to which you want to revert.

   In the **Actions** list, select **View Certificate Details** and confirm that you've selected the correct certificate. Then click **OK.**
3. In the **Actions** list, select **Revert to Default Certificate**.
4. When asked to confirm, click **Yes**.

   A dialog box informs you that the system has reverted to a self-signed certificate.
5. Click **OK**.
6. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.
7. After the system restarts, log back in, return to **Admin > Management and Security > Certificates**, and verify that the system has reverted to the default self-signed certificate:

   a. In the list of certificates, select the default certificate.

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

      The **Certificate Details** dialog box appears.

   c. Confirm from the information under **Issued To** and **Issued By** that the default self-signed certificate has replaced the CA-signed certificate.

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

Regenerating a Default Certificate

You need to update your certificate(s) whenever you make network configuration changes such as changing the host name or IP of your RealPresence Resource Manager system.

If you are using a default self-signed certificate, you can do this with the **Regenerate the Default Certificate** action.

To regenerate a self-signed certificate

1. Navigate to **Admin > Management and Security > Certificate Management**.
2. In the **Actions** list, select **Regenerate Default Certificate**.

   A new default certificate is generated.
3. Click **Restart to Apply Saved Changes**, and when asked to confirm that you want to restart the system so that certificate changes can take effect, click **OK**.
4. After the system restarts, log back in, return to **Admin > Management and Security > Certificates**, and verify that the system has reverted to the default self-signed certificate:
   - **a** In the list of certificates, select the default certificate.
   - **b** In the **Actions** list, select **Display Details**.

     The **Certificate Details** dialog box appears.
   - **c** Confirm from the information under **Issued To** and **Issued By** that the default self-signed certificate has replaced the CA-signed certificate.
5. Click **OK** to close the dialog box.

Revert to Legacy VVX Certificate

Some versions of the Polycom VVX rely on a self-signed certificate that comes installed with the RealPresence Resource Manager system.

The legacy self-signed certificate is deleted automatically when you import a CA certificate chain. However, if you need to revert to a self-signed certificate scenario for your systems, you will need to revert back to the **Legacy VVX Certificate.**

To revert to the Legacy VVX certificate

1. Navigate to **Admin > Management and Security > Certificate Management**.
2. Click **Revert to Legacy VVX Certificate**.

View Certificates and Certificate Details

To view the list of installed certificates

1. Navigate to **Admin > Management and Security > Certificate Management**.

   The **Certificate Management** page displays the list of currently installed certificates. By default, the system will display only one certificate. It will be identified as the **Resource Manager self-signed certificate**. When other certificates are installed, they will display along with the server identity certificate.

   The **Certificate Management** page has this information.

Column	Description
Status	The status of the certificate. Possible values include: • Certificate is valid • Certificate is invalid
Alias	The certificate name as assigned by the CA
Common Name	This is most often the fully qualified domain name of the server to which the certificate has been issued. If the certificate identifies a client (trusted peer) it might contain the name of a user or the name of an endpoint.
Purpose	The type of certificate. Possible values are: • RealPresence Resource Manager self-signed—the system identity certificate. • Trusted root certificate—the root certificate for a CA. • Intermediate certificate—certificate from an intermediate CA. • Trusted peer—certificate from any server or computer that is not a CA but whose identity is trusted.
Expiration	The expiration date of the certificate.

2. To view more information about a certificate, select the certificate and click **View Certificate Details**.

   The **Certificate Details** dialog box appears with this information.

Section	Description
Certificate Info	Purpose and alias of the certificate.
Issued To	Information about the entity to which the certificate was issued and the certificate serial number.
Issued By	Information about the issuer.
Validity	Issue and expiration dates.

Section	Description
Fingerprints	SHA1 and MD5 fingerprints (checksums) for confirming certificate.
Public Key	The certificate's public key, which in the public key infrastructure is distributed widely, and is not kept secure.

3 Use the arrows to reveal or hide information. Click **Close** when you are done.

View the Expiration Dates for Certificates

Certificates and certificate revocation lists expire. To view their expiration dates, see Create a Certificate Signing Request on page 351.

Configuring OCSP Settings

The RealPresence Resource Manager system supports using OCSP to verify the status of a certificate. This is an alternative to manually uploading CRLs (Certificate Revocation Lists). If your network does not include an OCSP responder, the RealPresence Resource Manager system parses individual certificates for a CRL Distribution Point URL. There is no need to upload a CRL to complete your certificate validation.

When configuring the RealPresence Resource Manager system to use an OCSP responder, you can either use the default OCSP information that is included in the certificates you receive or explicitly define the OCSP responder location. You should only define an explicit OCSP responder location if your deployment relies on a global OCSP responder.

To configure an OSCP settings for your certificate(s):

1 Go to **Admin > Management and Security > Certificate Management**.

2 Mark the **Enable OCSP** check box if your organization's PKI includes OCSP responders for revocation checking.

3 Use the **OCSP certificate** field to select one of the installed certificates to use to verify OCSP responses. Which certificate to use depends on your OSCP server configuration. Consult with your security administrator.

4 Depending on your security configuration, you can enter the URL of an **OCSP Responder** location to use.

During first-time setup, it is recommended that you leave this field blank. This can ensure that you don't have connection problems during initial configuration.

➢ If OCSP is enabled and NO responder URL has been specified:

- If the certificate contains an OCSP URL it will be used to check revocation. The OCSP URL is found in the certificate's AIA field.
- If the certificate doesn't contain the OCSP URL then if the certificate contains a CDP it will be used to check revocation.
- If the certificate doesn't contain a CDP revocation check fails and certificate isn't trusted.

- ➢ If OCSP is enabled and a global responder URL has been specified the global responder is used to check revocation.
  - ♦ If the global responder cannot be contacted then if the certificate contains a CDP it will be used to check revocation.
  - ♦ If the certificate doesn't contain a CDP revocation check fails and the certificate isn't trusted.

5 Click **Verify OCSP Configuration**.

The RealPresence Resource Manager system verifies that the OSCP configuration is correct. If the OSCP URL as well as the OSCP certificate, the configuration will also be verified as correct.

6 Click **Save OCSP Configuration**.

The RealPresence Resource Manager system saves this configuration.

7 After making any changes, you must reboot the system.

Understanding System Administration

This chapter describes the Polycom® RealPresence® Resource Manager system **Dashboard**, menu, and actions. It includes these topics:

- System Dashboard on page 360
- Dashboard Buttons on page 360
- Dashboard Panes on page 361
- System Administration Menu on page 367

System Dashboard

When you log into the RealPresence Resource Manager system with **Administrator** role and permissions, the system first displays the system **Dashboard**. Use the system **Dashboard** to view information about system health and activity levels.

> Polycom recommends that you use a minimum monitor display of 1280 x 1024 pixels to view the system **Dashboard**.

The system **Dashboard** displays data in an array of charts, forms, data grids, and other graphical displays. It is supremely customizable. You can modify your system **Dashboard** layout by moving (select the pane title, hold, drag and drop), minimizing, maximizing, closing, and restoring panes. Also note that your changes to the system **Dashboard** are persistent not just for a session but between logouts and logins.

Dashboard Buttons

In general, the system **Dashboard** displays information only. However, the following buttons are available from the **Dashboard** view.

Button	Use this button to....
Add Panes	Add additional display panes to the system **Dashboard**. See Dashboard Panes on page 361.
Refresh	Update the page with current information. To change the frequency of automatic screen refreshes from the default of 5 seconds, click the down arrow and select another option: 15, 30 45, or 60 seconds. The Refresh button flashes when the system refreshes the **Dashboard** or when you click **Refresh**.
Restart	Restarts the system. See Restart or Shut Down a Polycom RealPresence Resource Manager System on page 29.
Shutdown	Shuts down the system. See Restart or Shut Down a Polycom RealPresence Resource Manager System on page 29.

Dashboard Panes

By default the system **Dashboard** displays the following informational panes:

- Users Logged In on page 361
- Resource Manager Configuration on page 362
- Resource Manager Info on page 362
- Resource Manager Licenses on page 363

But you can add or remove panes to customize the system **Dashboard**. Additional panes that you can add include:

- Pre-call Status on page 364
- Today’s Adhoc Conferences on page 364
- Today’s Scheduled Conferences on page 364
- Endpoints on page 365 (multiple, configurable panes)
- Systems on page 365
- Conference Status on page 366
- Failed Enterprise Directory Login Attempts on page 366
- Redundancy Status on page 366
- MCU Status on page 366 (multiple, configurable panes)

These panes are described in more detail in the following topics.

Users Logged In

The **Users Logged In** pane displays the type and number of users that are currently logged into the system. A sparkline presents the number of logins over time (30 minutes total; updated every 5 minutes so there are 6 data points on the sparkline) for each user type.

The system identifies three user types by their permissions: **Administrators**, **Operators**, and **Schedulers**.

Note that these three user types are not necessarily the same as user roles. For example, users assigned the default **Administrator** and default **Device Administrator** roles appear in this pane as **Administrators**. And users assign the default **View Only Scheduler**, default **Scheduler**, and default **Advanced Scheduler** roles appear in this pane as **Schedulers**.

For more information, see Working with Management Roles and Permissions on page 281.

Resource Manager Configuration

The **Resource Manager Configuration** pane displays information about the configuration of the Resource Manager system, including:

Field	Description
Software Version	Displays the current version of the software running on the system.
Hardware Version	Identifies the Dell hardware version of the system.
CMAD Shipped Version	Displays the version of CMA Desktop for PC that shipped with the version of system software running on the system. Users can download this version of the Polycom CMA software from the **Downloads** page.
CMAD Mac Shipped Version	Displays the version of CMA Desktop for MacIntosh that shipped with the version of system software running on the system. Users can download this version of the Polycom CMA Desktop software from the **Downloads** page.
Enterprise Directory	Displays the enterprise directory configuration. Possible values include: • **Auto**—If the system is configured to auto-discover the enterprise directory server. • DNA name or IP address of the enterprise directory server—If an enterprise directory server is specified on the system configuration page. • **None**—If the system is not integrated with an enterprise directory server.
Database	Displays the database source (**Internal** or **External**) and the DNS name or IP address of the database server.
Time Source	Displays the time server source (**Internal** or **External**) and the IP address of the time server.
Redundancy	Displays 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**.
Remote Alerts	Displays whether or not the system is configured to send remote alert notifications.
Enterprise Directory DC	If the system is integrated with a domain controller for single sign on authentication, displays the domain name for that domain controller. If the system is not integrated with a single sign on domain controller, this field displays **Disabled**.
Remote Desktop	Displays whether or not Remote Desktop Connection is enabled.

Resource Manager Info

The **Resource Manager Info** pane displays general information about the system, including:

Field	Description
CPU Utilization	Displays two views of the system control processor unit (CPU) usage: • A sparkline that presents the CPU usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline) • A percentage indicator that shows the current usage
Paging File	Displays two views of the system paging file usage: • A sparkline that presents the paging file usage over time (10 minutes total; updated every 1 minute so there are 10 data points on the sparkline) • A percentage indicator that shows the current usage
Last JServer Start Time	
Provisioning in Progress	Displays the number of scheduled endpoint provisioning processes that are currently underway.
Software Updates in Progress	Displays the number of scheduled endpoint software update processes that are currently underway.
Total Memory	The total amount of RAM on the system.
Free Memory	The amount of free RAM space on the system.
Partition	The amount of used and unused capacity on the system partition.
Partition	The amount of used and unused capacity on the system partition.
Partition	The amount of used and unused capacity on the system partition.
Temperature	Temperature status information provided by the Polycom-branded Dell server agent through its MIB.
Power Supply Status	Power supply status information provided by the Polycom-branded Dell server agent thought its MIB.
Battery Status	Battery status information provided by the Polycom-branded Dell server agent thought its MIB.
Cooling Fan	Fan status information provided by the Polycom-branded Dell server agent thought its MIB.

Resource Manager Licenses

The **Resource Manager Licenses** pane displays information about how the system is licensed, including:

- The **Total Number of Licenses** available on the system
- The **Licenses in Use**, which displays two views of the system active calls:
  - A sparkline that presents the license usage over time (60 minutes total; updated every 5 minutes so there are 12 data points on the sparkline).
  - A percentage indicator that shows the current usage.

Pre-call Status

The **Pre-call Status** pane displays information about the next conference or conferences that are scheduled to launch including:

Field	Description
Time to Conference	Displays the system-defined pre-call status reporting time of 10 minutes. In other words, the Pre-call Status pane always reports on conferences that are scheduled to start in the next 10 minutes.
Scheduled to Launch	Displays the number of conferences scheduled to start in the next 10 minutes.
Ready to Launch	Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests that the system executes before launching a conference.
Ready to Launch with Device in Call	Displays the subset of conferences that are scheduled to start in the next 10 minutes and that have passed the resource tests but that still have one or more devices in another call.
NOT Ready to Launch	Displays the subset of conferences that are scheduled to start in the next 10 minutes but that have not yet passed the resource tests. Also displays the conferences that are not ready to launch.

Today’s Adhoc Conferences

The **Today’s Adhoc Conferences** pane displays information about the ad hoc conferences started by video endpoints registered to the Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of ad hoc conferences that were **Completed** for the current day
- The number of ad hoc conferences that are **Active** at the current time
- A bar chart that displays the number of ad hoc conferences (vertical axis) plotted against time of day (horizontal axis)

> **Note**
>
> Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager. Monitoring information will be incorrect and inconsistent.

Today’s Scheduled Conferences

The **Today’s Scheduled Conferences** pane displays information about the scheduled conferences managed by the Resource Manager system. For the current day (starting at 0:00 and ending at 24:00), it displays:

- The number of scheduled conferences that were **Completed** that day
- The number of scheduled conferences that are **Active** at the current time
- The number of scheduled conferences that are yet to occur (**Future**)

- A bar chart that displays time on the linear axis plotted against the number of scheduled conferences on the horizontal axis

Endpoints

The system allows you to add multiple **Endpoints** panes so you can create your own scheme for grouping and monitoring endpoints. When you add an **Endpoints** pane, you can give the pane a meaningful name and select which endpoints to monitor. You can save the pane, create others as needed. You can also reconfigure an **Endpoints** pane using the configuration tool.

Endpoints panes display the following information:

- The number of endpoints being monitored
- The number of monitored endpoints that are **In a Call**
- The number of monitored endpoints that are **Online**
- The number of monitored endpoints that are **Offline**

In addition, the **Endpoints** pane identifies any monitored endpoints that are experiencing alert conditions. If you click on an endpoint in the list, the system displays the **Endpoint > Monitor View**.

Finally, click **View Endpoint** to see the **Status**, **Name**, **Alias**, **IP Address**, **Owner**, and **Site** for the monitored endpoints. This status information is sent by the endpoints to the Resource Manager system.

Systems

The **Systems** pane displays summary information about the devices registered with the RealPresence Resource Manager system, including:

Field	Description
Endpoints	The number of endpoints registered with the RealPresence Resource Manager system.
VVXs	The number of VVX systems registered with the RealPresence Resource Manager system.
MCUs	The number of MCUs registered with the RealPresence Resource Manager system.
Gatekeepers	The number of gatekeepers identified to the RealPresence Resource Manager system.
Gateways	The number of individual H.323 cards and/or IP blades in Polycom MCUs are assigned the device type of GW/MCU during registration.
Rooms	The number of rooms defined with the RealPresence Resource Manager system.
SBCs	The number of Acme SBCs defined with the RealPresence Resource Manager system.
VBPs	The number of Polycom VBPs defined with the Resource Manager system.
DMAs	The DMA defined with the RealPresence Resource Manager system.
Touch Controls	The number of Touch Controls defined with registered endpoints.
RPADs	The number of RealPresence Access Directors provisioned by the RealPresence Resource Manager.

If any of the devices registered with the RealPresence Resource Manager system experience a fault, the **Systems** pane also displays an alert icon. Click the alert icon to see the **Endpoint** or **Network Device** view and get more information about the alert.

Conference Status

The **Conference Status** pane displays the list of active conferences. (see screen shot) plus 2 of 6 participants online.

Click on conference title to go to conference monitor view for that conference

Failed Enterprise Directory Login Attempts

The **Failed AD Login Attempts** pane displays:

- The total number of **Failed Logins** for Active Directory users in the last 24 hour period.
- The domain\username for the Active Directory users whose login attempts failed and how many times they failed. Click the domain\username to view the date and time for the failed attempts.

Redundancy Status

The **Redundancy Status** pane displays information about the Resource Manager system redundancy configuration, including:

- Whether or not the system is configured for redundancy. Possible values for Status are **Configured** or **Not Configured**.
- The **Virtual IP Address** for the redundant system. If it is not configured for redundancy, the value will be **No**.
- The IP address of the **Active Server**
- The IP address of the **Backup Server**

MCU Status

The system allows you to add multiple **MCU Status** panes so you can create a pane for all or individual MCUs registered with the Resource Manager system. When you add an **MCU Status** pane, you can give the pane a meaningful name and either select an MCU to monitor or select All MCUs. You can save the pane, create others as needed. You can also reconfigure an **MCU Status** pane using the configuration tool.

The **MCU Status** pane for **All MCUs** displays the following information:

Note

If your system has areas enabled, you will only be able to view MCUs that belong to areas that you have been assigned to manage.

Field	Description
Errors	Displays the cumulative number of alarms for all of the registered MCUs.

Field	Description
Warnings	Displays the cumulative number of warnings for all of the registered MCUs.
Active Conferences	Displays the total number of active conferences being hosted by all of the registered MCUs.

The **MCU Status** pane for an individual MCU displays the following information:

Field	Description
Errors	Displays the number of alarms on the MCU.
Warnings	Displays the number of conferences that are active on the MCU at the current time.
Active Conferences	Displays the number of active conferences currently being hosted by the MCU.
Number of Audio Ports	Displays the number of dedicated audio ports configured on the MCU.
Audio Ports Utilization	Displays two views of the MCU audio port usage: • A sparkline that presents the audio port usage over time • A percentage indicator that shows the current usage
Number of Video Ports	Displays the number of video ports configured on the MCU.
Video Ports Utilization	Displays two views of the MCU video port usage: • A sparkline that presents the video port usage over time • A percentage indicator that shows the current usage
Expected Port Utilization	A timeline that shows how many ports are scheduled for conferences within the next 45 minutes.

This status information is sent by the MCU to the Resource Manager system.

In addition, the **MCU Status** pane identifies when the monitored MCU is experiencing alert conditions.

System Administration Menu

The system **Admin** menu gives users with administrative permissions access to the day-to-day management tasks they need to monitor, maintain, and troubleshoot the Resource Manager system. Besides the **Dashboard**, it lists these selections:

Selection	Use this selection to...
Direct Conference Templates	Manage (add, edit, and delete) direct conference templates. See Direct Conference Templates on page 389.
Conference Settings	Enable or disable Conference Auto-launch and Conference Time Warning. See Conference Settings on page 393.
Provisioning Profiles	Manage (add, edit, and delete) dynamic or scheduled provisioning profiles.

Selection	Use this selection to...
Software Updates	Manage (add, edit, and delete) dynamic or scheduled software update packages.
Rooms	Manage (add, edit, and delete) rooms in the Resource Manager system directory.
Areas	Manage Areas for a Resource Manager system.
Directories	Manage the directories available to the Resource Manager system including the enterprise directory, address books, or Global Address Book.
Server Settings	Configure the basic Resource Manager system, which includes the network, system time, database, directory, licensing, redundancy, branding, GAB, remote alert, and E-mail set up.
SNMP Settings	Manage SNMP messaging for the Resource Manager system.
Management and Security	Upgrade the Resource Manager system and configure the certificate, security, and endpoint management set up.
Topology	Edit the default Resource Manager system **Site Topology** settings (which includes the definition of sites, site links, network clouds, and territories) to support your network topology and video call routing.
Alert Settings	Configure the Resource Manager system to send E-mail alerts for specified system or endpoint events.
Backup System Settings	Download a .zip archive file containing all configuration information necessary to restore the system.
Uploads	Upload SIP URI data to the Resource Manager system.
Troubleshooting Utilities	Access all of the troubleshooting information and utilities the Resource Manager system has available.
Report Administration	Configure report administration settings including retention periods, etc.

Setting Up Site Topology

This chapter describes how to edit the default Polycom® RealPresence® Resource Manager system topology settings to support your company's site topology. It includes these topics:

Site Topology Set Up

Note

If your RealPresence Resource Manager system is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the RealPresence Resource Manager. Be sure to consult with your DMA system admin before making any changes, see Considerations for Site Topology on page 265.

Site topology information describes your network and its interfaces to other networks, including the following elements:

- **Site** — A local area network (LAN) that generally corresponds with a geographic location such as an office or plant. A site contains one or more network subnets, so a device's IP address identifies the site to which it belongs.
- **Network clouds** — A Multi-protocol Label Switching (MPLS) network cloud defined in the site topology. An MPLS network is a private network that links multiple locations and uses label switching to tag packets with origin, destination, and quality of service (QOS) information.

  Note that MPLS clouds are not associated with an IP address ranges, so they can be used to group multiple subnets. They could also represent a service provider.

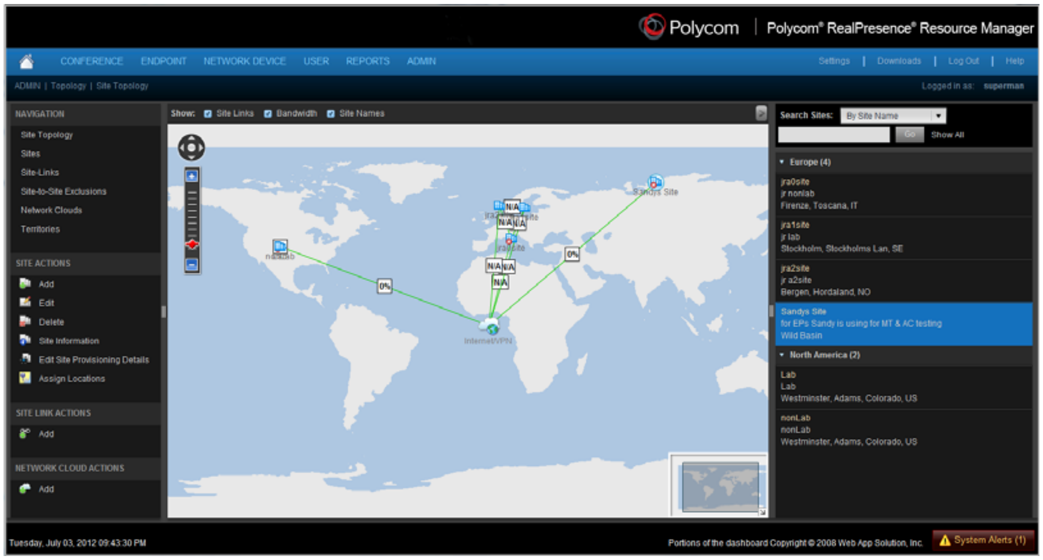
  While links to MPLS clouds have bandwidth and bit rate limitations, the cloud is infinite. In this way, clouds reflect the way in which businesses control bandwidth and bit rate.
- **Internet/VPN** — A entity that represents your network's connection to the public Internet.
- **Site link** — A network connection between two sites or between a site and an MPLS network cloud.

- **Site-to-site exclusion** — A site-to-site connection that the site topology doesn't permit an audio or video call to use.
- **Territory** — A grouping of one or more sites for which a Resource Manager system is responsible.

The site topology you create within the RealPresence Resource Manager system should reflect your network design. Consider the following information and best practices when creating your site topology:

- If your RealPresence Resource Manager is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the Resource Manager. Be sure to consult with your DMA system admin before making any changes, see Considerations for Site Topology on page 265.
- If possible, connect all sites to an MPLS cloud. MPLS clouds are like corporate networks, used to connect multiple subnets in multiple sites, but all servicing a company.
- Avoid cross loops or multiple paths to a site; otherwise a call may have different paths to a single destination. The more cross, circular, and multi paths you have, the higher the number of calculations for a conference.
- Link sites that aren't connected to an MPLS cloud directly to another site that is connected to an MPLS cloud. Do not create orphan sites.
- Calls are routed through a bridge, so bandwidth and bit rate limits for the site and subnet apply to all calls made using that bridge.
- Reserve the Internet/VPN "site" for IP addresses that fall outside your private or corporate network (for example remote workers), because all calls routed to the Internet/VPN site will be routed through the site on your private or corporate network that has Internet access.

The RealPresence Resource Manager system site topology function uses a dynamic, embedded mapping tool that graphically displays the sites, clouds (network and Internet), and site links (site-to-site or site-to-cloud) in your network.



Within this global and graphical view of the video conferencing network, you can:

- Create and link up to 500 sites
- Zoom and pan to view specific network components
- View system and device alarms
- View the video network capacity for sites and site links as indicated by the color and shape of its icons.
- Filter the view by site name, territory name, IP address, network devices, and alerts

Sites List

The **Sites** page (**Network Topology > Sites**) contains a list of the sites defined to the Resource Manager system.

Use the commands in the **Actions** list to add a site, edit or delete existing sites, and see information about a site, including the number of devices of each type it contains.

The following table describes the fields in the **Sites** list.

Column	Description
Name	Name of the site.
Description	Description of the site.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
Max Bandwidth (Mbps)	The total bandwidth limit for audio and video calls.
Max Bit Rate (Kbps)	The per-call bandwidth limit for audio and video calls. **Note** Bit rate is not the same as bandwidth. Since the bit rate applies in both directions and there is overhead, the actual bandwidth consumed is about 2.5 times the bit rate.
Territory	The territory to which the site belongs, which determines the Resource Manager system responsible for it.
Area	Available only when areas are enabled. The area to which the site is assigned. A user can only view area-specific information for an area(s) that he has permission to manage.

Add/Edit Site Dialog Box

Use the **Add Site** dialog box to define a new site in the system’s site topology and specify which subnets are associated with it. Use the **Edit Site** dialog box to redefine information for an existing site.

The following table describes the fields in the **Add Site** and **Edit Site** dialog boxes.

Field	Description
General Info	
Site Name	A meaningful name for the site, this name can be 64 characters(ASCII only) long.
Description	A brief description (ASCII only) of the site.
Site with RPAD	Indicates that a RealPresence Access Director is used for this site.
Enable Mutual TLS	Enable Mutual TLS
Override ITU Dialing Rules	Check this box to override the standard dial rules established by the International Telecommunications Union.
PBX Access Code	The access code required to enter the site's PBX system.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
# of Digits in Subscriber Number	The number of digits in a phone number. For example, in the United States, subscriber numbers may have seven digits or ten digits depending upon the region.
Assignment Method	The ISDN number assignment method for the site. Possible values include: • **No Auto Assignment**. Select this option when ISDN numbers are not assigned to IP devices. • **DID (Direct Inward Dial)**. Select this option when you assign a range of phone numbers received from the telephone company service. • **Gateway Extension Dialing**. Select this option when you have a single gateway phone number and a range of extensions (E.164 aliases) that are internal to the company. In this case, calls go through a gateway. Endpoints are differentiated by the extension at the end of the dial string. When a site is assigned an automatic assignment method, devices without an ISDN number are assigned one when they register. These numbers allow inbound calls to reach specific video endpoints. After an ISDN number is assigned to an endpoint, it is reserved for use as long as that endpoint remains registered with the RealPresence Resource Manager system. **Note** If you do not assign ISDN numbers automatically, you cannot call IP-only endpoints through an ISDN line.
Territory	Assigns the site to a territory, and thus to a RealPresence Resource Manager system.
Location	Specify the geographic location of the site either by longitude+latitude or country+city.

Field	Description
Assigned Area	Available only when areas are enabled. The area to which the site is assigned. A user can only view area-specific information for an area(s) that he has permission to manage.
Total Bandwidth (Mbps)	The total bandwidth of the pipe at the site.
Call Max Bit Rate (kbps)	The maximum bandwidth that can be used for each intrasite call at the site. The default and maximum value is 2000000 (2 GB).
ISDN Number Assignment— Assignment Method = 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— Assignment Method = 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.
H.323 Routing	
Internet calls are not allowed	Disables call routing through the Internet.

Field	Description
Allowed via H.323 aware firewall	Enables call routing through the Internet, using an H.323-aware firewall. **Notes** • For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string. • If you select **Allowed via H.323 aware firewall** you must create a site link between this site and the Internet/VPN site.
Allowed via H.323 aware SBC or ALG	Enables call routing via the Internet, using an H.323-aware SBC (Session Border Control) or ALG (Application Level Gateway) server. **Note** For an outbound call to the Internet, you must enter the firewall gateway service (for example, a Polycom VBP appliance) code before the IP address in the dial string.
Call Signaling IP Address	IP address of the SBC or ALG server. Supports only IPv4 addresses.
Port	Port address of SBC or ALG server.
Send Unmodified Dial String to SBC/ALG	Select this option if your SBC or ALG requires that the original dial string is passed to it. For example, an H.323 Annex O dial string such as user@company.com is passed directly to the SBC or ALG instead of resolving company.com to an IP address. Deselect this option if your equipment requires a dial string that is converted from company.com to gatekeeper IP address. This option is appropriate for the Polycom VBP.
SIP Routing	
Internet calls are not allowed	Disables call routing through the Internet.
Allowed via SIP aware firewall	Enables call routing through the Internet, using an SIP-aware firewall. **Notes** • For an outbound call to the Internet, you must enter the firewall gateway service (e.g. a Polycom VBP appliance) code before the IP address in the dial string. • If you select **Allowed via SIP aware firewall** you must create a site link between this site and the Internet/VPN site.
Allowed via SIP aware SBC or ALG	Enables call routing via the Internet, using an SIP-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 (for example, a Polycom VBP appliance) code before the IP address in the dial string.
Call Signaling IP Address	IP address of the SBC or ALG server. Supports only IPv4 addresses.

Field	Description
Port	Port address of SBC or ALG server.
Subnets	
Subnet IP Address/Mask	Specifies the subnets within the site. For each subnet, include: • IP Address range • Subnet mask • Maximum bandwidth for the subnet • Maximum bit rate per call for the subnet **Notes for sites that include a RealPresence Access Director system** If this site is used for a site that includes a RealPresence Access Director system, be sure to include the subnet where the RealPresence Access Director system resides.
Enterprise Directory Settings— **Endpoint Enterprise Directory security group settings**	
Universal Security Group Filter	When in secure mode, search and select groups that are provisioned to the endpoints to represent the valid lists of users that can log in as a user or administrator. If a user is not a member of one of the selected groups then the user is denied access to the endpoint.
Enterprise Directory Admin Group	
Enterprise Directory User Group	

Site Links

The **Site Links** page lists the links defined in the site topology. A link can connect two sites, or it can connect a site to an MPLS network cloud (see "Network Clouds" on page 102).

Use the commands in the **Actions** list to add, edit, or delete a site link. See Add/Edit Site Link Dialog Box on page 375 for a description of the fields in the site list.

Add/Edit Site Link Dialog Box

Use the **Add Site Link** dialog box to define a new site link in the Resource Manager system's site topology. Use the **Edit Site Link** dialog box to redefine an existing site link. A site link can connect two sites, or it can connect a site to an MPLS network cloud.

The following table describes the fields in the **Add Site Link** and **Edit Site Link** dialog boxes.

Field	Description
Name	A meaningful name for the site (up to 128 characters).
Description	A brief description of the site (up to 200 characters).
From site	The originating site of the link. The drop-down list includes all defined sites and the Internet. Can't be changed for a site-to-cloud link.
To site	The destination site of the link. The drop-down list includes all defined sites and an Internet/VPN option. Can't be changed for a site-to-cloud link.

Field	Description
Total bandwidth (Mbps)	Specifies the total bandwidth limit for this link.
Call Max bit rate (kbps)	Specifies the per-call bandwidth limit for this link.

Site-to-Site Exclusions

The **Site-to-Site Exclusions** page contains a list of the direct site-to-site connections that the system won't permit a call or session to use.

Use the commands in the **Actions** list to add and delete site-to-site exclusions. The following table describes the fields in the list.

Column	Description
From/To Site	Name of one of the two sites connected by the excluded link.
To/From Site	Name of the other site.

Territories

The **Territories** page contains a list of the territories defined in the site topology. On the right, it displays information about the selected territory.

A territory is a set of one or more sites for which a RealPresence Resource Manager system is responsible. By default, there is one territory named **Default Resource Manager Territory**, and its primary node (the Resource Manager system responsible for it) is set to this system.

You should configure the Resource Manager Default territory to be the primary DMA node AFTER you integrate with a DMA system.

Use the commands in the **Actions** list to add, edit, or delete a territory. See Add/Edit Territory Dialog Box on page 376 for a description of the fields in the territory list.

Add/Edit Territory Dialog Box

Use the **Add Territory** dialog box to define a new territory in the RealPresence Resource Manager system's site topology. Use the **Edit Territory** dialog box to define a new territory in the RealPresence Resource Manager system's site topology.

The following table describes the fields in the **Add Territory** and **Edit Territory** dialog boxes.

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

Field	Description
Primary Node	The primary node of the RealPresence Resource Manager system responsible for this territory. You can assign this territory to either a RealPresence Resource Manager or a DMA system. When integrating with a DMA system, enter the management FQDN or IP address of the cluster that will manage this territory. You should do this step AFTEr you integrate with a DMA system.
Backup Node	The second node, if any, of the RealPresence Resource Manager system responsible for this territory. You can assign this territory to either a RealPresence Resource Manager or a DMA system. When integrating with a DMA system, enter the management FQDN or IP address of the backup cluster that will manage this territory.
Associated Sites	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each currently belongs. Select a site and click the right arrow to move it to the Selected Sites list.
Selected Sites	Lists sites selected and shows the territory, if any, to which each currently belongs.

Network Clouds

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

Use the commands in the **Actions** list to add, edit, or delete an MPLS cloud. See the Cloud Info section of the Add/Edit Network Cloud Dialog Box on page 377 for a description of the fields in the **Network Clouds** list.

Add/Edit Network Cloud Dialog Box

Use the **Add Network Cloud** dialog box to define a new MPLS network cloud in the Resource Manager system's site topology. Use the **Edit Network Cloud** dialog box to redefine an existing MPLS network cloud.

The following table describes the fields in the **Add Network Cloud** and **Edit Network Cloud** dialog boxes.

Field	Description
Cloud Info	
Name	A meaningful name for the cloud (up to 128 characters).
Description	A brief description of the cloud (up to 200 characters).

Field	Description
Linked Sites	
Search Sites	Enter search string or leave blank to find all sites.
Search Result	Lists sites found and shows the territory, if any, to which each belongs. Select a site and click the right arrow to open the **Add Site Link** dialog box.
Selected Sites	Lists sites linked to the cloud and shows the territory, if any, to which each belongs.

Managing Sites

Site operations include:

- View the Graphical Site Topology on page 378
- View the Sites List on page 379
- Add a Site on page 379
- View Site Information on page 380
- Assign Locations to a Site on page 380
- Edit Site Settings on page 381
- Delete a Site on page 382

For information on editing a network provisioning profile, see Network Provisioning Profiles on page 185

View the Graphical Site Topology

To view the graphical site topology

» Go to **Network Topology > Site Topology**.

The **Site Topology** page appears. It graphically displays the sites and site links defined to the RealPresence Resource Manager system.

- ➢ Hover over a map element to view information about it.
- ➢ Use the slider bar to zoom in or out on the map.
- ➢ Select or deselect elements (**Site Links**, **Bandwidth**, or **Site Names**) to change what is displayed on the map.
- ➢ Use the **Select Sites** drop-down list to filter (by site name, territory name, IP address, network devices, and alerts) which sites are displayed on the map.

View the Sites List

To view the Sites list

» Go to **Network Topology > Sites**.

The **Sites** list appears. It includes this information:

Column	Description
Name	Name of the site.
Description	Description of the site.
Country Code	The country code for the country in which the site is located.
Area Code	The city or area code for the site. Do not include a leading zero. For example, the city code for Paris is 01; however, enter 1 in this field.
Max Bandwidth (Mbps)	The total bandwidth limit for audio and video calls.
Max Bit Rate (Kbps)	The per-call bandwidth limit for audio and video calls.
Territory	The territory to which the site belongs, which determines the Resource Manager system responsible for it.
Area	Available only when areas are enabled. The area to which the site is assigned. A user can only view area-specific information for an area(s) that he has permission to manage.

Add a Site

To add a site

1 Go to **Network Topology > Sites** or **Network Topology > Site Topology**.

2 In the **Sites** list or **Site Topology** page, click **Add Site**.

3 In the **Add Site** dialog box, enter a **Site Name** and **Description** for the site.

4 Complete the **General Info**, **Routing**, **Subnet**, and if applicable **ISDN Number Assignment,** sections of the **Add Site** dialog box. The minimum information required is **Site Name**, **Description**, **Location**, and **Subnets**.

For information about all of the site fields, see Add/Edit Site Dialog Box on page 371.

5 Click **OK**.

View Site Information

To view information about an existing site

1. Go to **Network Topology > Sites** or **Network Topology > Site Topology**.
2. In the **Sites** list or **Site Topology** page, select the site of interest and click **Site Information**.

   The **Site Information** dialog box displays the following site information.

Column	Description
Name	Name of the site.
Description	Description of the site.
Location	The specified location of the site identified either by longitude + latitude or by country + city.
Bandwidth (Mbps)	The specified total bandwidth limit for audio and video calls.
Bandwidth Used	Identifies the percentage of the maximum bandwidth currently occupied with audio and video calls.
Device Types	Identifies the type (Bridges, DMAs, VBPs, and Endpoints) and number of devices assigned to the site.
Alarms	Identifies the device alarms present within the site. Alarm information includes Status, Device Name, Device Type, and Description. Click **Details** to view more device details.
Subnets	Identifies the subnets within the site. Subnets information includes Bandwidth Used, Subnet (name), and (maximum) Bandwidth.

Assign Locations to a Site

Location has not always been a required field for sites. If your existing sites do not include location information, use the **Assign Locations** action to update your sites.

To assign a location to an existing site

1. Go to **Network Topology > Sites** or **Network Topology > Site Topology**.
2. Click **Assign Locations**.
3. In the **Assign Locations to Sites** dialog box, select the site of interest by marking the associated check box and click **Specify Location**.
4. To specify a location by city name:

   a. From the **Enter Location By** drop-down list, select **Search for City**.

   b. If you know it, select the **Country** name for the location.

   c. Enter the name of the **City** and click **Search**.

      The system returns the list of cities that match your entry.

- **d** Select the appropriate city using the **Country**, **Division**, and **Subdivision** fields to identify it and click **Select**.

5 To specify a location by latitude and longitude in decimal degrees format:

- **a** From the **Enter Location By** drop-down list, select **Latitude/Longitude (Decimal format)**.
- **b** Enter the **Latitude** and **Longitude** coordinates in decimal degrees (for example, Baltimore has a latitude of 39.3° and a longitude of 76.6°).
- **c** Enter a **Location Name**. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
- **d** Select the **Country** name for the location and click **Select**.

  The system uses the coordinates you input to place the site in the proper location on its site topology map.

6 To specify a location by latitude and longitude in DaysMinutesSeconds format:

- **a** From the **Enter Location By** drop-down list, select **Latitude/Longitude (DDD:MM:SS format)**.
- **b** Enter the **Latitude** and **Longitude** coordinates in the required format and select
- **c** Enter a **Location Name**. The system uses this location name for reference only; it does not validated the location name against the latitude and longitude coordinates that you enter.
- **d** Select the **Country** name for the location and click **Select**.

  The system uses the coordinates you input to place the site in the proper location on its site topology map.

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.
>
> If your RealPresence Resource Manager system is integrated with a Polycom DMA system, the DMA system inherits all site topology settings from the RealPresence Resource Manager system. Be sure to consult with your DMA system admin before making any changes, see Considerations for Site Topology on page 265.

To edit settings for a site

1 Go to **Network Topology > Sites** or **Network Topology > Site Topology**.

2 In the **Sites** list or **Site Topology** page, 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. For information about these sections, see Add/Edit Site Dialog Box on page 371.

4 Click **OK**.

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 **Network Topology > Sites** or **Network Topology > Site Topology**.
2. In the **Sites** list or **Site Topology** page, select the site of interest and click **Delete**.
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 calls (audio and video) that use the link. Links are bidirectional. After you have created a link from Site A to Site B, you automatically have a bi-directional link from Site B to Site A, although the link appears as unidirectional.

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.

Field	Description
Name	Name (ASCII only) of the inter-site link.
Description	Description (ASCII only of the inter-site link.
From Site	Identifies the first site to be linked. The drop-down list includes all defined sites and the Internet/VPN.
To Site	Identifies the other site to be linked. The drop-down list includes all defined sites and an Internet/VPN option.
Total Bandwidth (kbps)	The maximum available bandwidth for audio and video calls, which you set at the gateway or router.
Call Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call.

Site-link operations include:

- View the Site Links List on page 383
- Add a Site Link on page 383
- Edit a Site Link on page 383

- Delete a Site Link on page 384

View the Site Links List

To view the Site Links list

» Go to **Network Topology > Site-Links**.

The **Site-Links** list appears.

Column	Description
Name	Name of the link
Description	Description of the link
From Site	First site reached in the call route
To Site	Final site reached through this call link
Max Bandwidth	The maximum available bandwidth for audio and video calls, which you set at the gateway or router. Only applies to direct links.
Max Bit Rate (kbps)	The maximum bit rate allowed for an audio and video call. Only applies to direct links.

Add a Site Link

Before you can create a site link, you must add two or more sites to the system.

To add a site link

1. Go to **Network Topology > Site-Links**.
2. In the **Site-Links** page, click **Add**.
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. Enter the **Bandwidth** and **Max Bit Rate** and click **Save**.

   The new link appears on the **Site Links** page.

Edit a Site Link

You may need to edit site links 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 **Network Topology > Site-Links**.
2. In the **Site-Links** list, select the link of interest and click **Edit**.

3 In the **Edit Site-Link** dialog box, edit the **Name**, **Description, Bandwidth** or **Max Bit Rate**.

4 Click **Save**.

Delete a Site Link

You can remove site links from the Polycom Resource Manager system.

> **Note**
>
> Avoid removing a link on which a scheduled conference depends.

To delete a site link

1 Go to **Network Topology > Site-Links**.

2 In the **Site-Links** list, select the site link of interest and click **Delete**.

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

Site-to-Site Exclusions

Create site-to-site exclusions to explicitly deny connection between two sites for audio or video calls.

Site-link exclusion operations include:

- View the Site-to-Site Exclusion List
- Add a Site-to-Site Exclusion
- Edit a Site-to-Site Exclusion
- Delete a Site-to-Site Exclusion

View the Site-to-Site Exclusion List

To view the Site-to-Site exclusion list

» Go to **Network Topology > Site-to-Site Exclusion**.

The **Site-to-Site Exclusions** list appears.

Add a Site-to-Site Exclusion

Before you can create a site link exclusion, you must add two or more sites to the system.

Exclusions are by definition bilateral. No call traffic is allowed to flow across the site-link in either direction.

To add a site-to-site exclusion

1 Go to **Admin > Topology > Site-to-Site Exclusions**.

2 In the **Site-to-Site Exclusions** page, click **Add**.

3 In the **Add Site-to-Site Exclusions** wizard:

   a Select the first site of the **From/To** site pair (by clicking the appropriate button). If needed, use the **Search Site** field to find the site.

   b Select the second site of the **From/To** site pair (by enabling the appropriate check box) and click **Continue**. You can select more than one site, if needed.

   c Review the site-to-site exclusion and if it is correct, click **Save Exclusion**.

Edit a Site-to-Site Exclusion

You cannot edit a site-to-site exclusion; you can only delete it and then re-add it.

Delete a Site-to-Site Exclusion

To delete a site-to-site exclusion

1 Go to **Network Topology > Site-to-Site Exclusions**.

2 In the **Site-to-Site Exclusions** page, select the exclusion of interest and click **Delete**.

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

Territories

A territory is a set of one or more sites for which a RealPresence Resource Manager system is responsible. By default, there is one territory named **Default CMA Territory**, and its primary node (the RealPresence Resource Manager system responsible for it) is set to this system. For more information, see Territories on page 385.

You should configure the Resource Manager Default territory to be the primary DMA node AFTER you integrate with a DMA system.

Territory operations include:

- View the Territory List on page 385
- Add a Territory on page 386
- Edit a Territory on page 386
- Delete a Territory on page 386

View the Territory List

To view the Territories list

» Go to **Admin > Topology > Territories**.

The **Territories** list appears.

Add a Territory

To add a territory

1. Go to **Network Topology > Territories**.
2. In the **Territories** page, click **Add**.
3. Complete the **Territory Info** and **Associated Sites** sections of the **Add Territories** dialog box. For information about these fields, see Add/Edit Territory Dialog Box on page 376.
4. Click **OK**.

You should configure the Resource Manager Default territory to be the primary DMA node AFTER you integrate with a DMA system.

Edit a Territory

To edit a territory

1. Go to **Network Topology > Territories**.
2. In the **Territories** page, select the territory of interest and click **Edit**.
3. Change the **Territory Info** and **Associated Sites** information of the **Add Territories** dialog box as needed. For information about these fields, see Add/Edit Territory Dialog Box on page 376.
4. Click **OK**.

Delete a Territory

To delete a territory

1. Go to **Network Topology > Territories**.
2. In the **Territories** page, select the territory of interest and click **Delete**.
3. Click **Yes** to confirm the deletion.

Network Clouds

To simplify the network topology, define network clouds to represents a hub with many sites connected to each other such as a private network or VPN.

Network cloud operations include:

- Multi-tenancy Considerations for Network Clouds on page 387
- View the List of Network Clouds on page 387
- Add a Network Cloud on page 387
- Edit a Network Cloud on page 387

- Delete a Network Cloud on page 388

Multi-tenancy Considerations for Network Clouds

When areas are enabled for your system, sites can be assigned to areas. You must be sure that each site within a network cloud belongs to the same area. View the Sites list to determine the area for a site, see View the Sites List on page 379.

View the List of Network Clouds

To view the Network Cloud list

» Go to **Network Topology > Network Clouds**.

The **Network Clouds** list appears.

Add a Network Cloud

To add a network cloud

1 Go to **Network Topology > Network Clouds**.

2 In the **Network Clouds** page, click **Add**.

3 In the **Cloud Info** section of the **Add Network Cloud** dialog box, enter a unique and meaningful **Name** and **Description** for the cloud.

4 To create a link between a site and the network cloud:

   a Click **Linked Sites**.

   b In the **Search Sites** field, enter all or part of the site name or location and click **Find**.

   The list of sites containing the search phrase appear in the **Search Results** column.

   c Select one or more sites to link with the network cloud and then click the right arrow to move them to the **Selected Sites** column.

5 Click **OK**.

Edit a Network Cloud

To edit a network cloud

1 Go to **Network Topology > Network Clouds**.

2 In the **Network Clouds** page, select the network cloud of interest and click **Edit**.

3 Edit the **Cloud Info** or to create a link between a site and the network cloud:

   a Click **Linked Sites**.

- **b** In the **Search Sites** field, enter all or part of the site name or location and click **Find**.

  The list of sites containing the search phrase appear in the **Search Results** column.

- **c** Select one or more sites to link with the network cloud and then click the right arrow to move them to the **Selected Sites** column.

4 Click **OK**.

Delete a Network Cloud

To delete a network cloud

1. Go to **Network Topology > Network Clouds**.
2. In the **Network Clouds** page, select the network cloud of interest and click **Delete**.
3. Click **Yes** to confirm the deletion.

Understanding Conference Templates and Settings

This chapter describes information about conference templates and settings within the Polycom® RealPresence® Resource Manager system. This chapter includes the following sections:

- Direct Conferences vs. Pooled Conferences on page 389
- Direct Conference Templates on page 389.
- Pooled (DMA) Conference Templates on page 392
- Conference Settings on page 393, are global system-wide settings that apply to all scheduled conferences.

> The RealPresence Resource Manager systems does not support scheduling direct conferences on third-party MCUs. Template settings apply only to the RMX and MGC devices.

Direct Conferences vs. Pooled Conferences

The RealPresence Resource Manager system allows you to use two types of Future (scheduled) conferences: direct conferences and pooled conferences.

- **Direct Conferences** end on Polycom RMX systems, Polycom Collaboration Servers, or Polycom MGC systems that are managed by the RealPresence Resource Manager system. Users with the administrator role need to import direct conference MCU templates that can be used for direct conferences.
- **Pooled Conferences** end on resources managed by the Polycom DMA system (pool orders). Conference templates for pooled conferences are created and maintained on the DMA system.

Direct Conference Templates

Direct conference templates are based on existing conference profiles that have been created on the MCU. You can choose to have the template automatically synchronized with its associated RMX profile by maintaining the routing name of the RMX profile or download the profile directly to the RealPresence Resource Manager system.

Users assigned the **Administrator** role can add **Direct Conference Templates** from any MCU that is managed by the RealPresence Resource Manager system. They can also identify (by user role) which users have access to which **Direct Conference Templates**. Conference schedulers can then select from the different templates available to them to switch between different combinations of conference settings.

You create a direct conference templates in two ways:

- Standalone Templates: Download a conference profile from a managed MCU creating a "standalone" (free-standing) template independent of the profiles available on the system's RealPresence Collaboration Servers, Polycom RMX systems, or Polycom MGC systems.
- Linked Templates: Link the template to a RealPresence Collaboration Server or RMX profile that exists on some or all of the MCUs.

  Linked conference templates are not supported for Polycom MGC systems.

Conference templates for Pooled Conferences are created and managed on the Polycom DMA system.

For more information about the RMX profile settings, see the *Polycom® RMX® 1500/2000/4000 Administrator's Guide.*

Standalone Templates

Standalone templates defined in the RealPresence Resource Manager system free you from having to ensure that the exact same conference profiles exist on all the MCUs.

When it uses a standalone template for a conference, the system sends the specific properties to the MCU instead of pointing to one of its profiles.

Considerations for Polycom MGC Systems

Standalone or "downloaded" templates are the only ones allowed for use with Polycom MGC systems.

In addition, the RealPresence Resource Manager system does not support MGC templates that use the following dual stream settings: **Hi-Res Graphics or Live Video** setting.

Linked Templates

Linking a template to a RealPresence Collaboration Server or RMX profile ensures that the template's properties are in sync with the capabilities on the selected MCU.

When you use a linked template for a conference, you must also select the specific MCU that contains the profile on which the template is linked.

When you link a template to a profile, it's up to you to ensure that the profile exists on the MCUs you want to use with that template and that its settings are the same on all of them.

If do not select the MCU from which the template is based, the scheduled conference will not launch.

As a best practice, when linking templates to MCU profiles, this will make it easier for conference schedulers to select the bridge that corresponds with the template.

This option is not supported for MGC conference profiles.

Direct Conference Template Considerations for Multi-Tenancy

- When areas are enabled, the templates available for a given conference depend on the area to which the conference owner belongs. Only templates belonging to the same area as the conference owner are available to use when scheduling a conference.
- When areas are enabled, be sure to give your area-specific names to your templates. This is particular helpful if you have schedulers who have been given permission to manage more than one area.

Direct Conference Template Best Practices

The RealPresence Resource Manager system has a **Default Template**. Administrators with **Conference Setup** permissions can some settings of the template.

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.
- The template names **Default Template** and **Default Audio Templates** are stored in the system database and their names are not localized into other languages. If you wish to localized their names into your language, edit the templates and enter new names for them.

  When creating new direct conference 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).
- As a best practice, when linking templates to MCU profiles, this will make it easier for conference schedulers to select the bridge that corresponds with the template.

Multi-Tenancy Consideration

If your RealPresence Resource Manager system has areas enabled, be sure to give your area-specific names to your templates. This is particular helpful if you have schedulers who have been given permission to manage more than one area.

Pooled (DMA) Conference Templates

Both Pooled Conferences and Anytime Conferences are enabled when your RealPresence Resource Manager system is integrated with a Polycom DMA system. These conference types use conference templates that are created and managed in the Polycom DMA system.

This section includes the following topics:

- DMA System Conference Templates for Multi-Tenancy on page 392

- Establish Naming Conventions for DMA System Templates on page 392
- Considerations for Anytime Conference Templates on page 392

DMA System Conference Templates for Multi-Tenancy

DMA system conference templates cannot be assigned to a specific area. Area schedulers will be able to select from a list of all DMA system templates, regardless of the area to which they manage. You should implement a template naming convention to indicate to an area scheduler which DMA templates apply to his purview; for example, ***area1_template***.

Establish Naming Conventions for DMA System Templates

By default, all DMA system conference templates are made available to conference schedulers who have permission to create pooled conferences and anytime conferences. To differentiate which DMA system conference templates should be used for which conferences, you should implement a naming convention that informs the scheduler which conference template is appropriate.

Anytime Conference Templates

For example, you could prefix a template designed for use with anytime conferences with the word “anytime”; for example, **anytimeconf_standard**, **anytimeconf_autoterminate**, **anytimeconf_nochair**, and so on.

Considerations for Anytime Conference Templates

An anytime conference is initiated when the first person calls into the conference and triggers the hosting bridge to dial-out to the remaining conference participants.

Once an Anytime conference is configured, conferences can be started at any time by authorized participants. The following events occur when a new Anytime conference is added:

- A participant with scheduling permissions creates a new Anytime conference and the conference is assigned a virtual meeting room (VMR) number.
- An **Chairperson passcode** is automatically generated and may be required to launch an Anytime conference (depending on your conference template).The owner receives the owner passcode needed to launch the conference via the meeting e-mail.
- Depending on the conference template settings, all dial-out participants are automatically called either when first participant dials the VMR number or the conference owner dials the VMR and enters the owner passcode.
- If the conference template requires a chairperson, dial-in participants are placed on hold until someone dials in and enters the chairperson passcode.
- The conference continues until all participants hang up the call, unless your template includes an auto-terminate setting.

Configure Auto-Terminate

Anytime conferences do not have designated start and end times. As a result, the conference may be left open and the VMR in use if the last caller does not hang up. You can mitigate this occurrence by configuring the DMA conference template to use an RMX profile that has Auto-Terminate enabled.

For more information about RMX profiles and how to use an existing RMX profile for a DMA conference template, see *Polycom DMA 7000 System Operations Guide*.

Initiate Conference Dial-out

You can configure the DMA system conference template to define who can trigger the dial-out to participants. You use the **Conference requires chairperson** setting to determine when dial-outs are initiated. Remember to use an intuitive naming convention for DMA system conference templates.

- When you enable the **Conference requires chairperson** setting, the dial-out process will begin when the chairperson dials into the conference. An example name for a template with this setting could be **Anytime Conference - Chair Starts Dial-Outs**.
- If you leave this check box unmarked, the dial-out process will begin when the first person dials into the conference. No chairperson passcode is needed. An example name for a template with this setting could be **Anytime Conference - 1st Dial-in Starts Dial-Outs**.

Conference Settings

Conference settings apply to conferences scheduled using the RealPresence Resource Manager system. These settings include:

Field	Description
Conference Time Warning	Specifies whether or not the Polycom Resource Manager system sends a message to video endpoints in a conference to warn the endpoint users that their conference is scheduled to end soon. The system sends the message 17 minutes, 10 minutes and 5 minutes before the conference is scheduled to end. To support this feature, the video endpoint system must be capable of receiving a system **Send Message** action. By default, **Conference Time Warning** is enabled. **Note** This feature is not related to the MCU-based **End Time Alert Tone** feature. **Pooled Conferences** This setting does not apply for Pooled Conferences.
Automatically Include Conference Owner (Scheduler) in New Conferences	Select this option when you wish the system to always include the person scheduling the conference as a conference participant. Do not select this option if your organization has assistants or operators schedule conferences for others.

Field	Description
Allow overbooking of dial-in participants	Select this option to allow schedulers to schedule dial-in participants to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference
Conference and chairperson passcode length	Designate the required length of the system-generated conference and chairperson passcodes. The acceptable length for both of these passcodes is 6 to 16 characters. By default, the required length for both of these passcodes is set to 15 characters. **Note** • Depending on the system settings, the scheduler may be allowed to change the conference or chairperson passcode. However, the passcode length requirement still applies. • If an administrator changes the passcode length here at the same time a scheduler edits the passcode settings for a scheduled conference, the scheduling operation may use either the old or the new length, depending on the exact timing.

Setting Up Conference Templates and Settings

This chapter includes information about adding direct conference templates and conference settings within the Polycom® RealPresence® Resource Manager system. It includes these topics:

View the Direct Conference Templates List

You can view a list of added direct conference templates.

To view the Direct Conference Template list

1. Go to **Conference > Direct Conference Templates**.

   The **Direct Conference Templates** list appears.

2. Click a template from the list to view its settings.

   You can expand the settings descriptions in the right pane of the screen.

Add a Direct Conference Template

When you add a template to the RealPresence Resource Manager from an MCU, you can use it for conferences you want to schedule. You can add direct conference templates from any MCU that is managed by the RealPresence Resource Manager system.

To add a direct conference template

1. Go to **Conference > Direct Conference Templates**.
2. On the **Direct Conference Templates** list, click **Add**.
3. In the **Select an MCU** dialog box, choose an MCU from which to add a template and click **View Profile.**
4. In the **Select a Profile** dialog box, choose an MCU conference profile to add as a template.
   - ➢ To link the template to its MCU profile, click **Use Routing Name**.

     For more information, see Linked Templates on page 390

     This option is not supported for MGC conference profiles.
   - ➢ To create a standalone template, click **Download Profile**.
5. In the **Add Direct Conference Template** dialog box, you can customize the profile summary.

Field	Description
General Settings	
Name	Enter a unique and meaningful name for the template, which can be up to 50 characters long.
Description	Enter a meaningful description (ASCII only) of the conference settings template.
Audio-Only Template	Select this option to designate the template as an audio-only template. Selecting this option disables many settings.
Supported MCUs	Specify the supported MCU type. Possible values include: • RMX • MGC • RMX + MGC
Always Use MCU	When selected, an MCU is used for the scheduled conference, regardless of the number of participants. When not selected, an MCU is used only when necessary.
Dial Options	These settings apply only to video conferences. The video dial options are: • **Dial-In Only** (all participants dial into the conference) • **Dial-Out Only** (all participants are called by the system) • **Dial-In + Dial-Out** (The person setting up the conference can specify which participants must dial into the conference and which participants are called by the system.)
Assign Area	Select an area to which to assign this template. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.
Template will be available to users with the selected roles...	Select the roles to which users must be assigned for them to see this template when scheduling conferences.

Field	Description
Available Roles	The list of roles defined to the RealPresence Resource Manager system.
Selected Roles	The list of roles that can use the conference template being defined.

6 Click **OK**.

The new template appears in the **Direct Conference Template** list.

> The RealPresence Resource Manager 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 or endpoints.

Edit a Direct Conference Template

To edit a conference template

1 Go to **Conference > Direct Conference Templates**.

2 On the **Direct Conference Templates** list, select the template of interest and click **Edit**.

3 Edit the **Customized Profile Summary** as needed.

4 Click **OK**.

Delete a Direct Conference Template

To delete a conference template

1 Go to **Conference > Direct Conference Templates**.

2 On the **Direct Conference Templates** list, select a template and click **Delete**.

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

Set Conference Settings

To specify conference settings

1 Go to **Conference > Conference Settings**.

2 On the **Conference Settings** page, make the required selections. Conference Settings on page 393.

3 Click **Update**.

Disable Conference Time Warning

To disable the conference time warning

1 Go to **Conference > Conference Settings**.

2 In the **Conference Time Warning** section of the **Conference Settings** page, clear the **Enabled** check box.

3 Click **Update**.

Overbooking Dial-in Participants

A user with the administrator role can configure the system to allow scheduler’s to overbook dial-in participants. In this case, dial-in participants can be scheduled to dial into multiple conferences, but the system reserves resources for the participant for only the first scheduled conference. Dial-out participants cannot be scheduled into multiple conferences.

To allow schedulers to overbook dial-in participants

1 Go to **Conference > Conference Settings**.

2 In the **Allow Overbooking of dial-in participants** section of the **Conference Settings** page, check the **Enabled** check box.

3 Click **Update**.

Add Customized Text to E-mail Notifications

To add customized text to all conferencing E-mail notifications

1 Go to **Admin > Server Settings > E-mail**.

2 In the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page, type in the introductory text you want to appear at the start of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.

3 In the **Text at the End of the Reminder E-mail** section of the **E-mail** page, type in the closing text you want to appear at the end of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.

4 Click **Update**.

Edit Customized Text in E-mail Notifications

To edit the customized text in all conferencing E-mail notifications

1. Go to **Admin > Server Settings > E-mail**.
2. To change the introductory text, replace the text in the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page with the new text you want to appear at the start of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
3. To change the closing text, replace the text in the **Text at the End of the Reminder E-mail** section of the **E-mail** page with the new text you want to appear at the end of all conferencing E-mail notifications.

   This text field is limited to 650 characters. The text you type here will appear in plain text just as you typed it.
4. Click **Update**.

Delete Customized Text in E-mail Notifications

To delete the customized text in all conferencing E-mail notifications

1. Go to **Admin > Server Settings > E-mail**.
2. To delete the introductory text, select the text in the **Text at the Beginning of the Reminder E-mail** section of the **E-mail** page and press DELETE.
3. To delete the closing text, select the text in the **Text at the End of the Reminder E-mail** section of the **E-mail** page and press DELETE.
4. Click **Update**.

Understanding Directories

This chapter describes the Polycom® RealPresence® Resource Manager system enterprise directory integration and operations. It includes these topics:

- Directory Management Overview on page 400
- Directory Management Supported Configurations on page 400
- RealPresence Resource Manager System and Windows Authentication on page 406
- Managing Directories on page 408
- Endpoint Directory and Directory Settings on page 412

Directory Management Overview

In a large organization, integrating your RealPresence Resource Manager system with Microsoft Active Directory greatly simplifies the task of managing conference system security. Directory management provides the following features.

- Single sign-on capability. Users get the benefits of pass-through authentication, allowing them to leverage their Active Directory user name and password to login to the Polycom CMA Desktop system. This happens without the user having to enter their credentials, creating seamless integration for logins.
- Single management environment. After the initial setup of the RealPresence Resource Manager system, adding groups into RealPresence Resource Manager system is no more complex than adding a group to a file share or database. Continue to manage your group memberships through Active Directory, then grant those groups rights within the RealPresence Resource Manager system.
- Allows you to continue leveraging the existing role-based security model that you have in place, though the RealPresence Resource Manager system only uses Universal groups.

Directory Management Supported Configurations

There are many possible configurations available within Microsoft Active Directory, some of which are not fully supported by the RealPresence Resource Manager system. These topics describes the implications of different Microsoft Active Directory configurations for integrating with the RealPresence Resource Manager system.

Multiple Forests

Microsoft Active Directory may be set up in either a single-forest or multi-forest configuration. However, the RealPresence Resource Manager system requires that user accounts reside in a single forest.

Multiple Domains

Microsoft Active Directory forests may contain one or more domains. In either configuration, the directory must have a Global Catalog service. The RealPresence Resource Manager system can integrate to either single or multiple domains, so long as they reside in the same forest structure.

Microsoft Active Directory domains are organized into trees, each tree being a group of domains which share a consistent DNS namespace (ex: polycom.com and na.polycom.com would be in the same tree, while polycom.com and resouceManagerDevelopment.net would be separate trees, if they were in the same forest). The RealPresence Resource Manager system will integrate to all domains in a multi-tree forest.

Viable options:

1. Integrate to all domains of a multi-domain forest configuration.
2. Restrict to a single domain tree in a multi-domain forest through the use of LDAP Search baseDN criteria.

Groups

Microsoft Active Directory provides three group scopes: Universal, Global, and Domain Local. Both Global groups and Universal Groups are held on all Global Catalog servers in the forest. The RealPresence Resource Manager system supports only the Universal groups.

Microsoft Active Directory provides two group types: Security and Distribution. The RealPresence Resource Manager system supports either of these group types.

> An Active Directory forest with a functional level of Windows 2000 Mixed mode only supports Universal Distribution groups. Windows 2000 Native mode, Windows 2003 Mixed, and Windows 2003 forest functional levels support Universal Security and Distribution groups.

In addition to leveraging Active Directory Universal groups, the RealPresence Resource Manager system also has Local groups, which you can use to grant a standard set of rights to multiple users or groups. These RealPresence Resource Manager system Local groups can have as members, RealPresence Resource Manager system Local users, Active Directory users or Active Directory Universal groups. In this fashion, you can nest a variety of users and groups into a RealPresence Resource Manager system Local group and assign those users rights through their RealPresence Resource Manager system Local group membership, simplifying management of rights on the RealPresence Resource Manager system.

Users

The RealPresence Resource Manager system supports both local and enterprise user accounts. Local user accounts exist entirely on the RealPresence Resource Manager system. They can be created and managed whether or not the system is integrated to an enterprise directory. Enterprise user accounts exist in your enterprise Active Directory. The RealPresence Resource Manager system cannot create or manage Active Directory accounts, except to modify their privileges on the RealPresence Resource Manager system itself.

If simultaneously using local and enterprise accounts, it is important to avoid duplication of account data. For example, if your Active Directory has a user named John Doe with a username of jdoe, a local account for this user must possess a unique name, such as localjdoe or johndoetest. If duplicate user accounts exist in the same domain or across domains, the user associated with these accounts will not be able to log into a dynamically managed endpoint.

The RealPresence Resource Manager system accesses the enterprise directory in a read-only mode. It does not create, modify, or delete Active Directory users or groups in any way.

Once you integrate with an enterprise directory, it's best to minimize your dependency on local users. A single local administrative user account must exist, and it should be used only when there is a problem connecting to the enterprise directory.

This configuration provides flexibility and varying security levels as follows:

- Restricted access: For security reasons, local user accounts do not have access to any data in Active Directory, though they can see the Active Directory users and groups as defined in the RealPresence Resource Manager system's security.
- Administration: Active Directory users and their Active Directory group memberships are managed through your Active Directory. RealPresence Resource Manager system local users are managed through the RealPresence Resource Manager system's web interface.
- Security: Local accounts have their own passwords, which are stored on the RealPresence Resource Manager system. Active Directory user accounts maintain the same users' Active Directory credentials and password complexity policies, which are validated by the domain controllers.

How Global Catalog Searches Work

When you integrate the RealPresence Resource Manager system with Active Directory, you can configure it to integrate in one of two ways:

- It can access a specific global catalog server by host name or IP address (not recommended, due to a lack of redundancy).

  If you select this option, the domain name that you specify for the RealPresence Resource Manager system must match the DNS name suffix of the Global Catalog server (example: dc1.polycom.com configured as the Global Catalog, then you must enter polycom.com as the domain name of the RealPresence Resource Manager system server).
- It can auto-discover the server by querying the DNS for the closest Global Catalog server (strongly recommended).

  If you select this option, you can specify any domain in the Active Directory forest in the Domain Name criteria for the RealPresence Resource Manager system server. The DNS server must contain Active Directory-specific entries.

  It is recommended that you enter the forest root DNS domain name.

When configured to auto-discover the server, every time the RealPresence Resource Manager system needs to bind to a Global Catalog server for LDAP queries, the RealPresence Resource Manager system performs the following.

- Uses Microsoft's LDAP Ping mechanism to determine the site in which the system is located.
- Uses a DNS SRV record query to find a Global Catalog server within the same site.
- Connects to the Global Catalog on the domain controller and queries for the object in question and any relevant information (such as GUID, userID, name, phone number).

You can secure the connection between the RealPresence Resource Manager system and the Active Directory server's Global Catalog using **LDAP-S** (via outbound TCP/UDP port 3269) or **Start TLS** (via outbound 3268 TCP/UDP). To implement the secure connection, the appropriate ports must be open on any network equipment between the Global Catalog and the RealPresence Resource Manager system.

Accounts Required for the System

RealPresence Resource Manager System Service Account

Before integrating the RealPresence Resource Manager system with an Active Directory forest, you must create a service account for it in Active Directory. This service account is a read-only user account that the RealPresence Resource Manager system uses to perform LDAP queries against your Active Directory Global Catalog.

RealPresence Resource Manager System Computer Account

The RealPresence Resource Manager system requires a computer account to enable secure channel communications with the Active Directory forest that is being leveraged for authentication. This account must be pre-created and the password set by an administrator from a Domain Controller.

> When setting up a redundant RealPresence Resource Manager system, the redundant servers use the same computer account to create their secure channel connection. The computer account name does not have to match the host name of your RealPresence Resource Manager system server.

Understanding Base DN

When the RealPresence Resource Manager system is integrated with an enterprise directory, the system uses the baseDN to determine domains and manage directory searches.

The **Base DN** field is where you specify the *distinguished name* (DN) of a subset of the Active Directory hierarchy (a domain, subset of domains, or organizational unit) to which you want to restrict the RealPresence Resource Manager system search. It acts like a filter.

By default, the **Base DN** field is empty. The first time you tell the system to connect to the enterprise directory server, leave the **Base DN** field empty. Once you have established a working connection with your Active Directory, then you enter a **Base DN**.

The following table illustrates some basic examples of Base DN filter expressions.

Search baseDN expression	Description
(ou=ResourceManagerGroups,dc=example,dc=com)	Include only groups and users which reside within the ResourceManagerGroups OU in the example.com domain.
(dc=example,dc=com)	Include only groups and users which reside within the example.com domain or domain tree.

Expressions in the Base DN and exclusion filter fields must be formatted according to RFC-4514, section 2.4.

Some special characters are allowed in the **BaseDN** field. They include:

Character	Character Name
“ % ”	Percent
“ ”	Space
“ " ”	Double quote
“ ? ”	Question mark
“ { ”	Open brace
“ } ”	Close brace
“ ^ ”	Caret
“ ~ ”	Tilde
“ [”	Open bracket
“] ”	Close bracket
“ ‘ ”	Single quote
“ & ”	Ampersand
“ | ”	Pipe or bar

The special characters that are not allowed in the **Base DN** field without the special escape character (backslash, \) are:

Character	Character Name
“ \ ”	Backslash
“ = ”	Equal
“ , ”	Comma
“ # ”	Pound
“ + ”	Plus

Character	Character Name
“ ; ”	Semicolon
“ < ”	Less than
“ > ”	Greater than

Therefore, to use these character as part of a name, they must be preceded in the **Base DN** field by a backslash. For example, the baseDN of an ou named "`tom,ann,bob`" in the "myteam.example.com" domain must be entered as:

```
ou=tom\,ann\,bob\ dc=my team,dc=example,dc=com
```

Or the baseDN of an ou named "#+,=<>\ " in the "mydomain.example.com" domain must be entered as

```
ou=\#\+\,\=\<\>\\\ ,dc=mydomain,dc=example,dc=com
```

Note that this applies only to attribute values, not the `ou=` or `dc=` structure.

Understanding Exclusion Filters

Using LDAP exclusion filters, you can exclude objects in your directory based on a wide variety of criteria within your Active Directory environment. Any LDAP filters that you create must follow the LDAP standard and reference the LDAP display name of the attributes against which you are filtering.

The following table illustrates some basic examples of exclusion filter expressions.

Search baseDN expression	Description
Memberof=cn=Restricted Group,OU=users,dc=example,dc=com	Excludes all users who are members of “Restricted Group” within the Users OU in the example.com domain.
!(Memberof=cn=Video Users,OU=Users,dc=example,dc=com)	Includes only groups and users within the Video Users group in the Users OU in the example.com domain.

Creating exclusion filters can impact the performance of your LDAP queries. As a best practice, use indexed attributes and do not use medial searches when implementing exclusion filters. For more information, see Creating More Efficient Microsoft Active Directory-Enabled Applications.

The following table illustrates some more advanced examples of exclusion filter expressions.

Search baseDN expression	Description
!(| (memberof=CN=Sales,DC=europe,DC=example,DC=com)(memberof=CN=IT,DC=europe,DC=example,DC=com))	Includes only users that are members of the 'Sales' or 'IT' Groups in the domain europe.example.com. **Notes:** • The expression should be in continuous line with no carriage returns or extra spaces (not possible in this document's format). • By excluding an entity, we implicitly mean to include all other entities. Conversely, by including an entity, we are implicitly excluding all other entities. Hence, this exclusion filter will suffice for a case where, for example, the administrator wants to include Sales and IT but exclude Human Resources, Engineering, etc., within the specified domain.
&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2)	Excludes all users who are disabled. Note this is using a different but valid notation.

RealPresence Resource Manager System and Windows Authentication

To allow Microsoft Active Directory users with dynamically-managed endpoints to securely log into their endpoint without typing in their network credentials, the RealPresence Resource Manager system must be integrated with an Active Directory server and trusted by Active Directory.

When the RealPresence Resource Manager system starts up, it performs the following actions.

- Uses Microsoft's LDAP ping mechanism to determine the site in which the system is located.
- Uses a DNS SRV record query to find a domain controller within the same site.

When an Active Directory user attempts to log into the RealPresence Resource Manager system, it authenticates the user by connecting to the domain controller that it is connected to and passes the user's credentials using NTLMv2. The credentials are seamlessly passed to the RealPresence Resource Manager system utilizing a secure channel connection from the user's workstation, using the credentials with which they logged into the workstation.

> Because the RealPresence Resource Manager system uses NTLMv2, the password is not stored within and the RealPresence Resource Manager system never receives the user's password.

Some important notes about the RealPresence Resource Manager system Active Directory integration:

- The RealPresence Resource Manager system is not joined to the domain. Other computers on the network cannot browse its file system and it cannot be managed remotely by existing IT mechanisms such as SMS.
- The RealPresence Resource Manager system does not modify the Active Directory in any way.
- The RealPresence Resource Manager system can auto-discover the closest logical domain controller and Active Directory servers, but to do this the network DNS server must have a DNS SRV record for these servers. Once the domain controller's hostname and IP address have a record on the DNS, the RealPresence Resource Manager system can auto-discover the IP address of the domain controller. If your Active Directory does not publish the domain controller's hostname and IP address to the network DNS, you must edit the file to include it.
- The RealPresence Resource Manager system requires that you enable **Digitally sign communications** on the Active Directory server.

Generating E.164 Aliases

The RealPresence Resource Manager system generates E.164 aliases for registered endpoints. The alias it creates is based on the endpoint type, so that a single user with multiple endpoints can have multiple E.164 aliases.

> If a user is deleted from Active Directory, the E.164 alias for that user is not deleted and cannot be re-used.

Polycom CMA Desktop Clients

When a user of a CMA Desktop client successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that client. This alias is based on the user's phone number in Active Directory (or a random, unique number, if no phone number is listed for the user). Users of other endpoints can connect to the user's endpoint by dialing this alias or by searching for them by name in the directory.

Polycom HDX Systems

When a user of a Polycom HDX system successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that endpoint also. Again, this alias is based on the user's phone number in Active Directory (or a random, unique number, if no phone number is listed for the user), but with a “1” appended to the number. Users of other endpoints can connect to the user's endpoint by dialing this alias or by searching for them by name in the directory.

Polycom VVX Systems

When a user of a Polycom VVX system successfully logs into a RealPresence Resource Manager system, the RealPresence Resource Manager system creates an E.164 alias for that endpoint also. Again, this alias is based on the user's phone number in Active Directory (or a random, unique number, if no phone number is listed for the user), but with a “2” appended to the number. Users of other endpoints can connect to the user's endpoint by dialing this alias or by searching for them by name in the directory.

Managing Directories

This section describe the directory management operations. It includes these topics:

- Integrate with Enterprise Directory Server Option on page 408
- Allow Delegated Authentication to Enterprise Directory Server on page 411
- Remove or Include Dynamically-Managed Endpoints in the Global Address Book on page 413

Integrate with Enterprise Directory Server Option

The process of integrating with an enterprise directory server, involves these steps:

- Create the RealPresence Resource Manager System Service Account on page 409
- Create the RealPresence Resource Manager System Computer Account on page 409
- Enable Integration with the Enterprise Directory Server on page 410

Enabling the **Integrate with Enterprise Directory Server** option allows RealPresence Resource Manager system users who are included in the Active Directory to log into the RealPresence Resource Manager system interface using their network credentials.

Enabling the **Integrate with Enterprise Directory Server** option also allows endpoint users to select conference participants and rooms from the enterprise directory. Because endpoint connections to LDAP use the endpoint user’s credentials, the Active Directory access control lists identify which endpoint users and rooms each user can see.

> The RealPresence Resource Manager system supports only the Microsoft Active Directory for its enterprise directory.

In addition, administrative users can:

- View some enterprise user and group information
- Import enterprise groups into the RealPresence Resource Manager system
- Assign roles to users in different enterprise groups
- Identify enterprise resources, such as rooms, so that they can be treated as resources in the RealPresence Resource Manager system

> To allow endpoint users to use NTLM Single Sign On technology to connect to the RealPresence Resource Manager system, see Allow Delegated Authentication to Enterprise Directory Server on page 411.

For more information about Active Directory and LDAP, see MS Strategy for Lightweight Directory Access Protocol (LDAP).

Create the RealPresence Resource Manager System Service Account

To create the RealPresence Resource Manager system service account

1. On the Active Directory server, open the **Active Directory Users and Computers** module (**Start > Programs > Administrative Tools > Active Directory Users and Computers**).
2. Click the node for your domain and then right-click the OU folder in which you want to add a user account and select **New > User**.
3. At a minimum, in the **First name**, **Full name**, and **User logon name** fields, type `resoucemanagerservice` or an appropriate name for your environment and click **Next**.
4. In the **Password** and **Confirm Password** fields, type a password for the service account to use during initial integration. This is the password you must enter on the RealPresence Resource Manager system **Enterprise Server** page.
5. Select the **Password never expires** option, unselect the **User cannot change password** option, click **Next** and then **Finish**.

- You can reset the password for this account manually, but to do so you must change it in Active Directory first and then update the RealPresence Resource Manager system LDAP Server page.
- The service account requires the rights to read all properties on all users and groups that will be used in the RealPresence Resource Manager system. Without these permissions, it may not function properly.

Create the RealPresence Resource Manager System Computer Account

To create the RealPresence Resource Manager System computer account

1. On the Microsoft Active Directory system, open the **Active Directory Users and Computers** module (**Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Select the node for your domain, right-click the OU folder in which to add the computer account and then select **New > Computer**.
3. In the **Computer name** field, type *PolycomResourceManager* or an appropriate name for your environment and then click **Next** and **Finish** (or simply click **OK** depending on your version of Active Directory).
4. Ensure that the **Active Directory Users and Computer**s console will show all available computer options necessary for the remaining steps by enabling **View** > **Advanced Features**.
5. Right-click the computer account, select **Properties,** and then select the **Security** tab.
6. In the **Group or user names** section of the Security tab, select the **SELF** object.
7. In the **Permissions for SELF** section, select **Change password,** and then click **OK**.
8. Login to the domain controller where the computer account was created and set the password using the following command:

```
net user <computername>$ <password>
```

For example: `net user polycomresoucemanager$ p@ssw0rd`

- Performing the net user command on any machine other than a domain controller will not assign the computer account password for the RealPresence Resource Manager system computer account.
- At initial integration, the RealPresence Resource Manager system will change its Computer Account password to a random 120 character string including special characters. This password will also be changed, to a new randomly generated password, every time the RealPresence Resource Manager system is rebooted, or every week if no reboots are performed. Because this is a Computer account, resetting the password to a known value requires use of net user commands on an Active Directory Domain Controller.

Enable Integration with the Enterprise Directory Server

To integrate the RealPresence Resource Manager system to an enterprise directory server

1. Go to **Admin > Directories > Enterprise Directory**.
2. On the **Enterprise Directory** page, select **Integrate with Enterprise Directory Server**.
3. To have the system auto-discover the server by querying DNS, enable **Auto-discover** in the **Enterprise Directory Server DNS Name** section; otherwise, enter the **DNS Name** for the enterprise directory server.
4. As needed, configure these settings.

Setting	Description
Domain\Enterprise Directory User ID	Domain and Enterprise Directory User ID for an account that the RealPresence Resource Manager system can use to access the enterprise directory server and retrieve group, user, and room information. This is the account created Create the RealPresence Resource Manager System Service Account on page 409. This User ID must have read permissions so it can search the entire forest on the enterprise directory server. This User ID is automatically associated with the RealPresence Resource Manager system administrator role - by default it is the ONLY enterprise directory User ID with this role.
Enterprise Directory User Password	The password for the enterprise directory user account

Setting	Description
Security Level	The level of security on the connection between the RealPresence Resource Manager system and the enterprise directory server. Possible values include: • **Plain**—No security on the connection • **LDAPS**—The connection is secured over outbound port 3269 using LDAP-S in a manner similar to `https`. If the “Domain Controller: LDAP Server signing requirements” setting on the Active Directory server is set to “Require Signing”, then you must use LDAPS to secure the connection. • **StartTLS**—The connection is secured over outbound port 3268 (the same port as **Plain**), but it then negotiates security once the socket is opened. Some LDAP servers reject any unsecured transactions, so the first command is the `StartTLS` negotiation command.
Ignore Disabled Enterprise Directory Users	Check this field to have the RealPresence Resource Manager system ignore disabled enterprise users in its queries.
Enterprise Directory Exclusion Filter	If necessary and you understand the filter syntax, specify other types of user accounts to exclude. Don’t edit these expressions unless you understand LDAP filter syntax. For more information, see Understanding Exclusion Filters on page 405.
Enterprise Directory Search BaseDN	If necessary and you understand the filter syntax, specify the top level of the enterprise directory tree (referred to as the base DN) to search. Don’t edit these expressions unless you understand the filter syntax. For more information, see Understanding Base DN on page 403.

5 If you also wish to implement single sign-on, see the following section Allow Delegated Authentication to Enterprise Directory Server on page 411. Otherwise, click **Update**.

Allow Delegated Authentication to Enterprise Directory Server

The RealPresence Resource Manager system **Use Single Sign on (Integrated Windows Authentication)** option, allows endpoint users who are included in the enterprise directory to securely log into their dynamically-managed endpoint without typing in credentials.

> To allow RealPresence Resource Manager system users who enter their network usernames and passwords to log into the RealPresence Resource Manager system and select conference participants from your company’s active directory, see Integrate with Enterprise Directory Server Option on page 408.

To delegate authentication to the enterprise directory server

1 Go to **Admin > Directories > Enterprise Directory.**

2 On the **Enterprise Directory** page, select **Allow delegated authentication to enterprise directory server**.

3 To have the system auto-discover the closest logical domain controller and enterprise directory servers, in the **Domain controller name** section enable **Auto-discover**; otherwise, enter the fully qualified hostname of the domain controller (for example, `dc1.mydomain.com`).

> To auto discover the domain controller and enterprise directory server, the network DNS server must have a DNS SRV record for these servers.

4 Enter the **Username** (`domain\`<***computer name***>) and **Password** and click Update.

Endpoint Directory and Directory Settings

When an endpoint registers with the RealPresence Resource Manager 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. If an endpoint is configured to **Allow Directory Changes**, additions and deletions to the Global Address Book are pushed to the endpoint.

Endpoints that get their global directory from the RealPresence Resource Manager system will either get the Global Address Book or the enterprise LDAP directory. Two **Directory Setup** options allow you to affect which devices and users appear in the endpoint directory.

Typically, endpoints that do not use the RealPresence Resource Manager as register for the Polycom GDS and are listed in the RealPresence Resource Manager system Global Address Book. The Global Address Book allows standard endpoint users to call other standard endpoint users by selecting them by name. In this case, the Global Address Book is limited to 2000 entries, which is the limit that standard endpoint systems can manage.

> - The RealPresence Resource Manager system Global Address Book lists endpoints. Endpoints may or may not have users or rooms associated with them. On an endpoint, the Global Address Book does not list users unless they have endpoints associated with them.
> - If your company has more than 100 endpoints, don’t limit the Global Address Book on the endpoint side or the endpoint user won’t have access to all Global Address Book entries.
> - The RealPresence Resource Manager system Global Address Book does not support unicode data.

The **Include dynamically-managed devices in the Global Address Book** option changes the Global Address Book so that it also includes all dynamically-managed endpoints such as CMA Desktop and Polycom VVX 1500 endpoints in the Global Address Book. In this case, the Global Address Book limit is increased to 5000 entries. (Dynamically-managed endpoints are always included in the enterprise LDAP directory.)

By default the **Include dynamically-managed devices in the Global Address Book** option is selected. This brings all of your devices and users together into one endpoint directory. However, you may not want to take advantage of this feature if you have legacy endpoint systems such as VSX and FX endpoints. These endpoint systems cannot handle the increased size of the Global Address Book. For information on clearing this option, see Remove or Include Dynamically-Managed Endpoints in the Global Address Book on page 413.

The second **Directory Setup** option affects both the Global Address Book and the enterprise LDAP directory. The RealPresence Resource Manager system Guest Book includes static user entries. By selecting the **Show Guest Book entries in the Directory**, these static entries are included in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise LDAP directory. The **Show Guest Book entries in the Directory** option is also selected by default.

Remove or Include Dynamically-Managed Endpoints in the Global Address Book

By default the RealPresence Resource Manager system includes dynamically-managed endpoints in the Global Address Book. However, you may not want to take advantage of this feature if you have legacy endpoints such as VSX and FX endpoints. These endpoints may not be able to handle the increased size of the Global Address Book.

To remove enterprise users from the RealPresence Resource Manager system Global Address Book

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory** page, clear **Include dynamically-managed devices in the Global Address Book**.
3. Click **Update**.

To include enterprise users in the RealPresence Resource Manager system Global Address Book

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory** page, select **Include dynamically-managed devices in the Global Address Book**.
3. Click **Update**.

Remove or Include Guest Book Entries in the Directory

By default the RealPresence Resource Manager system includes Guest Book entries in the endpoint directory, regardless of whether the endpoint directory is the Global Address Book or the enterprise directory.

To remove Guest Book entries from the endpoint directory

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory Setup** page, clear **Show Guest Book entries in the Directory**.
3. Click **Update**.

To include Guest Book entries in the endpoint directory

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory Setup** page, select **Show Guest Book entries in the Directory**.
3. Click **Update**.

Allow Local Users to View Enterprise Directory Entries

You can allow local users to access Enterprise Directory entries when the RealPresence Resource Manager is integrated with an enterprise directory.

To allow local users to view Enterprise Directory Entries

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory Setup** page, mark the **Allow endpoint directories for local users to include enterprise directory user information** check box.
3. Click **Update**.

Support LifeSize Endpoints in Directories

You can include LifeSize endpoints in the endpoint directory by configuring your directory setup. When you do this, you also need to ensure that your LifeSize endpoint is configured to use the correct LDAP settings.

Complete the following steps:

- Modify Directory Listings on page 414
- Configure LDAP Settings on page 414

For more information about LifeSize endpoints, see Considerations for LifeSize Endpoints on page 113.

Modify Directory Listings

You need to allow your directory listings to include support for LifeSize endpoints.

To modify directory listings for LifeSize endpoint support

1. Go to **Admin > Directories > Directory Setup**.
2. In the **Directory Setup** page, mark the **Modify directory listings for LifeSize endpoint support** check box.
3. Click **Update**.

Configure LDAP Settings

In addition to configuring directory listing support in the directory set up, you need to also ensure that the LifeSize endpoint is configured to use the RealPresence Resource Manager system’s LDAP settings. You can provision these through a scheduled provisioning profile or configure them manually on the endpoint.

To add LDAP settings to a scheduled provisioning profile

1. Go to **Admin > Provisioning Profiles > Scheduled Provisioning Profiles**.
2. In the **Scheduled Provisioning Profiles** page, click Add.
3. In the **Add Profile** dialog box, select the **Endpoint Type** for the provisioning profile, enter a name for the profile, and click Next.
4. As needed, complete the various settings that you would like to provision for your LifeSize endpoint.

   For more information about these fields, see Endpoint Fields for Scheduled Provisioning on page 247.
5. For Directory support, select **the Directory > LDAP** page.
6. **On the Directory > LDAP page:**

   a. Mark the **Provision This Page** check box.

   b. In the **LDAP** field, select **Enabled** from the drop-down list.

   - In the **LDAP Username** field, enter **uid=ldapgab,ou=system**
   - In the **LDAP Password** field, enter the password for the Polycom Global Address Book if you have one. If not, leave this field blank.
   - In the **LDAP Base** field, enter **DC=Polycom,dc=com**
7. Click OK.

> If you manually enter the LDAP settings on the LifeSize endpoint, the value for the **LDAP Base** field needs to be the following: **OU=Endpoints,DC=Polycom,dc=com**.

Setting Up Directories

This chapter describes how to manage the Global Address Book in the Polycom® RealPresence® Resource Manager system. It includes these topics:

- View the Global Address Book on page 416
- Set or Change the GAB Password on page 417

View the Global Address Book

The Polycom Global Address Book is a system-managed endpoint directory that allows users with video endpoints to look up and call other users with video endpoints in their video communications network.

From a video endpoint system, users can locate other user's endpoints by name in the Global Address Book and initiate a call without knowledge of the other user's equipment. The RealPresence Resource Manager system will filter incompatible endpoints out of the Global Address Book (GAB) results so that the GAB presented to H.323-only endpoints will not include ISDN-only endpoints and the GAB presented to ISDN-only endpoints will not include H.323-only endpoints.

> Global Address Book filtering applies only to Polycom endpoints. The Global Address Book is not filtered on third-party endpoints.

For more information on the Global Address Book, see Endpoint Directory and Directory Settings on page 412.

To view the Global Address Book

1. Go to **Admin > Directories > Global Address Book**.
2. As needed, use the **Filter** to customize the **Global Address Book**. It can be filtered by **Endpoint Name, IP Address** or **Area**. This **Area** filter is only visible when Areas are enabled and the user manages more than one area. A user can only view area-specific information for an area(s) that he has permission to manage.

   The user information found in the **Global Address Book** includes:

Column	Description
Owner	The associated user or resource ID.
Name	The name of the registered endpoint.
GAB Display Name	The name of the registered endpoint as it will be displayed to other endpoint users. This display name is an ASCII only field.
IP Address	The IP address of the endpoint.
Alias	The alias associated with the endpoint.
Primary ISDN	The primary ISDN number for the endpoint (if any).
Secondary ISDN	The secondary ISDN number for the endpoint (if any).
Owner	The user associated with the endpoint.
Type	The type of the endpoint.
Area	The area in which the endpoint resides.

Set or Change the GAB Password

You can require that endpoints be provisioned with a password in order to access the Global Address Book on the RealPresence Resource Manager system. To do so, set a Global Address Book password as described here. Use the same procedure to change the Global Address Book password.

Note that even if the Global Address Book is password protected, some third-party endpoints may not be required to provide a password because they are not directory-password aware. They have unrestricted access to the Global Address Book.

To provision this password to endpoints, see Add a Scheduled Provisioning Profile on page 126.

To set or change the password for the Global Address Book

1. Go to **Admin > Directories > 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.)
4. Confirm the new password and click **Save**.

   Once you set this password, endpoints that are not provisioned with this password cannot access the Global Address Book on the RealPresence Resource Manager system.

Using Multiple Address Books

This chapter describes how to set up multiple address books in the Polycom® RealPresence® Resource Manager system. It includes these topics:

Multiple Address Books Overview

Users assigned the **Administrator** role can create multiple address books in the RealPresence Resource Manager system. Multiple address books are subsets of the Global Address Book (GAB) and let you manage which users (local and enterprise), endpoints, rooms, groups, and guests appear in each address book.

Multiple address books support both the Global Address Book and LDAP protocols. Endpoints requesting directory information using either protocol receive either the default address book or the address book assigned to the user's group.

If you do not want to use multiple address books, you can leave the default address book set to **All Entries**. Using this default, all users will see all entries in the directory. Be sure that all groups are assigned either the **System Default** or **All Entries** option. **System Default** is the default group setting.

An endpoint must be associated with a User and the User must be in a Group in order to specify an address book.

How Multiple Address Books Work

Use address books to limit access to people and endpoints. For example, you can set up separate address books for each department in your organization. Each address book would include only RealPresence Resource Manager system users in that department and only rooms in that department's location.

Users not assigned the Administrator or Area Administrator role (available if you have enabled areas) will not be aware of address books. They will see only those users (local and enterprise directory), endpoints, rooms, groups, and guests in the same address book that the user is assigned to.

For information about how address books work in a multi-tenancy environment, see Area Address Books on page 431.

To implement multiple address books, complete the following tasks

1. Add an Address Book on page 420

   RealPresence Resource Manager system users assigned the **Administrator** role can create address books and associate users (local and enterprise directory), endpoints, rooms, groups, and guests with one or more address books. This process controls where each entity appears as an address book entry.

2. Assign Address Books to Groups on page 424

   RealPresence Resource Manager system users assigned the **Administrator** role can assign an address book to a group. A group can be assigned to only one address book. This process controls the address book that users and endpoints have access to.

3. Change Address Book Priority on page 425

   RealPresence Resource Manager system users assigned the **Administrator** role can set the priority of address books. The priority affects which address book a user has access to. For example, if a user is a member of two different groups and each group is assigned a different address book, the user can access the address book that is higher in priority.

Address Book Considerations for Multi-Tenancy

If you have enabled the Areas feature, you can only associate users and endpoints that are in the same area that you have been assigned to manage.

Users not assigned the Administrator or Area Administrator role will not be aware of address books or be allowed to edit them. They will see only those users (local and enterprise directory), endpoints, rooms, groups, and guests in the same address book and area to which the user is assigned.

When you manage more than one area, you can create address books that contain users and endpoints from each area that you manage. However, users in that address book will only be able to view users from the area to which they also belong.

For more information about multi-tenancy, see Configuring Multi-Tenancy on page 428.

View the Address Book List and Details

To view the address book list and details

1 Go to **Admin > Directories > Address Books**.

The Address Book list appears, with details of the selected address book in the right pane.

Column	Description
Priority	The priority affects which address book a user sees. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority.
Address Books	Name of the address book.
Description	A brief description of the address book.
Area	This column is only available when areas have been enabled and indicates the area to which the address book belongs. You can view this column if you have the administrator role or have the area administrator role and manage more than one area. If the address book belongs to an area that you do not manage, the area name will be listed as “Restricted” as you do not have permission to view that area.

2 In the **Address Book Details** in the right pane, expand the tree to view the tiers along with users, endpoints, rooms, groups, and guests associated with the address book.

Add an Address Book

You can add many address books to the RealPresence Resource Manager system, and each address book can have up to 100 tiers.

Tiers are only meant to allow you to organize the address book contents. They will not be visible to endpoint users when they access the directory. Each tier can have up to three subtiers., and you can have address book entries at any tier level.

Associating users, endpoints, rooms, groups, and guests with an address book controls where these entities appear. For example, if you associate user A with address book A, the user will appear as an entry in address book A. You can associate any of these entities with more than one address book, and the entity will appear as entry in each address book.

Groups in the RealPresence Resource Manager system control the address book users, endpoints, and rooms have access to. To set which address book an entity has access to, see Assign Address Books to Groups on page 424.

To add an address book

1 Go to **Admin > Directories > Address Books**.

2 Click **Add**.

3 Complete the fields in the **Add an Address Book** dialog box.

Field	Description
Address Book Information	
Name	A meaningful name to identify this address book.
Description	A brief description of the address book.
Assign Area	You can assign an address book to an area you manage. This drop-down list is only available when areas are enabled. You can only view areas that you manage.
Address Book Tiers	
New Tier	Select where you want to add a tier and click to add a new tier to the address book.
Edit Tier Name	Select a tier and click to change a tier name.
Delete	Select a tier and click to delete a tier.

4 To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

a Search for the users you want to associate. Use the **Filter** to customize the list.

b Select the users you want and click **Specify Tier**.

c Select the tier you want for the users and click **OK**.

5 To associate endpoints with this address book, click **Associate Endpoint**s.

Only endpoints that are not associated with a RealPresence Resource Manager system user appear in the list.

a Use the **Filter** to customize the list.

The **Address Book/Tier** column shows all of the address books the endpoints appear in.

b Select the endpoints you want and click **Specify Tier**.

c Select the tier you want for the endpoints and click **OK**.

6. To associate rooms with this address book, click **Associate Rooms**.

   The **Address Book/Tier** column shows all of the address books the rooms appear in.

   a. Use the **Filter** to customize the list.
   b. Select the rooms you want and click **Specify Tier**.
   c. Select the tier you want for the rooms and click **OK**.

7. To associate groups with this address book, click **Associate Groups**.

   The **Address Book/Tier** column shows all of the address books the groups appear in.

   a. Use the **Filter** to customize the list.
   b. Select the groups you want and click **Specify Tier**.
   c. Select the tier you want for the groups and click **OK**.

8. To associate guests with this address book, click **Associate Guests**.

   The **Address Book/Tier** column shows all of the address books the guests appear in.

   a. Use the **Filter** to customize the list.
   b. Select the guests you want and click **Specify Tier**.
   c. Select the tier you want for the guests and click **OK**.

9. Click **OK**.

Edit an Address Book

You can edit an address book to add or remove users, endpoints, rooms, groups, and guests.

You can find any of these entities that are not currently associated with an address book by selecting **Current Association** from any **Filter**, then selecting **Not Associated With An Address Book**.

If a group is set up with the **Enterprise Directory Viewable** option not selected, you can still add that group to an address book. The group itself will not appear as an entry in the address book, but the members of the group will.

To edit an address book

1. Go to **Admin > Directories > Address Books**.
2. Select an address book.
3. Click **Edit**.
4. Edit the fields in the **Edit an Address Book** dialog box.

Field	Description
Address Book Information	
Name	A meaningful name to identify this address book.

Field	Description
Description	A brief description of the address book.
Assign Area	You can assign an address book to an area you manage. This drop-down list is only available when areas are enabled. You can only view areas that you manage.
Address Book Tiers	
New Tier	Select where you want to add a tier and click to add a new tier to the address book.
Edit Tier Name	Select a tier and click to change a tier name.
Delete	Select a tier and click to delete a tier.

5 To associate users with this address book, click **Associate Users**.

The **Address Book/Tier** column shows all of the address books the users appear in.

a Search for the users you want to associate. Use the **Filter** to customize the list.

b Select the users you want and click **Specify Tier**.

c Select the tier you want for the users and click **OK**.

d To delete a user from the address book, select the user and click **Delete**.

The user is removed from the address book, but remains in the RealPresence Resource Manager system.

6 To associate endpoints with this address book, click **Associate Endpoint**s.

Only endpoints that are not associated with a RealPresence Resource Manager system user appear in the list.

The **Address Book/Tier** column shows all of the address books the endpoints appear in.

a Use the **Filter** to customize the list.

b Select the endpoints you want and click **Specify Tier**.

c Select the tier you want for the endpoints and click **OK**.

d To delete an endpoint from the address book, select the endpoint and click **Delete**.

The endpoint is removed from the address book, but remains in the RealPresence Resource Manager system.

7 To associate rooms with this address book, click **Associate Rooms**.

The **Address Book/Tier** column shows all of the address books the rooms appear in.

a Use the **Filter** to customize the list.

b Select the rooms you want and click **Specify Tier**.

c Select the tier you want for the rooms and click **OK**.

   d To delete a room from the address book, select the room and click **Delete**.

      The room is removed from the address book, but remains in the RealPresence Resource Manager system.

8 To associate groups with this address book, click **Associate Groups**.

   The **Address Book/Tier** column shows all of the address books the groups appear in.

   a Use the **Filter** to customize the list.

   b Select the groups you want and click **Specify Tier**.

   c Select the tier you want for the groups and click **OK**.

   d To delete a group from the address book, select the group and click **Delete**.

      The group is removed from the address book, but remains in the RealPresence Resource Manager system.

9 To associate guests with this address book, click **Associate Guests**.

   The **Address Book/Tier** column shows all of the address books the guests appear in.

   a Use the **Filter** to customize the list.

   b Select the guests you want and click **Specify Tier**.

   c Select the tier you want for the guests and click **OK**.

   d To delete a guest from the address book, select the guest and click **Delete**.

      The guest is removed from the address book, but remains in the RealPresence Resource Manager system.

10 Click **OK**.

Assign Address Books to Groups

You can assign an address book to a group, but you cannot assign address books directly to users. Group assignment controls to which address book users and endpoints have access. Each group can have just one address book assigned to it, but users can be in more than one group.

Address book priority affects which address book users and endpoints can access. For example, if a user is a member of two different groups and each group is assigned a different address book, the user will see the address book that is higher in priority. To change priority, see Change Address Book Priority on page 425.

To assign an address book to a group

1. Go to **User > Groups**.
2. Select the group you want to assign.
3. Click **Edit**.
4. In the **Edit Local Group** dialog box, select address book you want from the **Assign Address Book** drop-down list.

5 Click **OK**.

Viewing the Address Book a User is Assigned To

You can see which address book a user is assigned to. The address book assignment controls the address book entries a user or endpoint can access.

To view the address book a user is assigned to

1 Go to **User > Users**.

2 Select the user you want.

3 Click **View Details**.

4 In the **View User** dialog box, click **Inherited Group Info**.

5 Click **OK**.

Delete an Address Book

You can delete an address book when it is no longer needed. Deleting an address book does not delete the users, endpoints, rooms, groups, or guests that were in the address from the RealPresence Resource Manager system.

Any entity that was assigned the deleted address book will have access to one of the following:

- Another address book if the entity is a member of another group that is assigned to an existing address book.
- The default address book.

To delete an address book

1 Go to **Admin > Directories > Address Books**.

2 Select the address book you want to delete.

3 Click **Delete**.

A confirmation message appears.

4 Click **Yes**.

Change Address Book Priority

You can change the priority of address books. The priority determines which address book a user sees. For example, if a user is a member of two different groups and each group is associated with a different address book, the user will see the address book that is higher in priority.

The **All Entries** address book always has the highest priority and **None** always has the lowest priority. If the address book for one of the groups the user belongs to is changed to **All Entries**, the user will see all entries regardless of the priority of the address book for the other group.

To change address book priority

1. Go to **Admin > Directories > Address Books**.
2. In the Priority column of an address book, enter the priority you want.

   Use only whole numbers and only numbers that fall within the total count of address books. For example, if you have four address books, only 1 through 4 are valid priority values.
3. Click **Update Priority**.

   The system changes the order of the address book list.

Set the Default Address Book

You can set the default address book. The default address book sets the address book all new users have access to if no address book is assigned through a group.

If you do not want to use multiple address books in the RealPresence Resource Manager system, leave the default address book set to **All Entries** (the default). Using this default, all users will be able to see all entries in the directory. Be sure that all groups are assigned either the **System Default** or **All Entries** option. **System Default** is the default group setting.

If you create multiple address books, you can change the default address book to one of the address books you created.

To set the default address book

1. Go to **Admin > Directories > Address Books**.
2. Click **Set Default**.
3. In the Default Address Book dialog box, select the option you want:
   - **All Entries**—Default setting. All users, endpoints, groups, rooms, and guests are in one address book and all have access to all address book entries.
   - **None**— No directory entries will be available.
   - **Specify**—Select the address book you want as the default.
4. Click **OK**.

Copy an Address Book

You can copy an existing address book as a shortcut to creating a new address book. The copy process can copy the entire address book or just the tier structure.

To copy an address book

1. Go to **Admin > Directories > Address Books**.
2. Select the address book you want to copy.
3. Click **Copy**.
4. In the **Copy Address Book** dialog box, select the option you want:
   - **Entire Address Book**—This option copies all of the tiers and the users, endpoints, rooms, groups, and guests that are associated with the address book to the new address book.

     If areas are enabled, the address is copied to the same area to which the initial address book belongs.
   - **Tiers only**—This option copies only the tier structure to the new address book.
5. Enter a meaningful **Name** and **Description**.
6. Click **OK**.

   You can now edit the new address book to add or delete entries.

Configuring Multi-Tenancy

The Polycom® RealPresence® Resource Manager system supports multi-tenancy with its areas feature. Multi-tenancy allows you to use the system to service multiple customers, internal or external. Each area serves a system tenant by partitioning off a collection of resources including users, associated endpoints, network devices, etc.

Administration and conferencing duties for areas can then be delegated to users within that area or by a set of super users who are allowed to view and manage all areas. You can set up flexible scenarios by having an area scheduler or area operator for each respective tenant or area. Otherwise, you can limit area administration tasks to users specifically allowed to manage that area.

For example, in an enterprise deployment, the RealPresence Resource Manager system administrator can divide up users and resources according to department and then delegate video conferencing duties to users within that area. This allows the system administration duties to remain with a specialized video IT department, while video conference scheduling can be delegated to users within specific areas. Areas also allow the administrator to run area-specific reports on how specific departments within the enterprise are utilizing video conferencing.

Note

The Areas feature of the Resource Manager system is a licensed feature. Contact your sales representative for more details.

Planning For Multi-Tenancy

You should plan your multi-tenancy environment so that you can ensure scalability and efficient use of resources. Setting up the Resource Manager system for multi-tenancy should use the following best practices:

- RealPresence Resource Manager system does not support integration with more than one Active Directory or multi-forest Active Directory integrations. If you need to support users that reside in different Active Directories or different Active Directory forests, you cannot use the Resource Manager system’s integration with Active Directory feature. You will need to use only local RealPresence Resource Manager system users. To save time, you can import users into your RealPresence Resource Manager system.
- Software updates cannot be assigned to an area.
- You must use dynamic provisioning when areas are enabled. Other methods of endpoint provisioning are not supported. See Using Admin Config Provisioning Profiles on page 245

- Polycom DMA systems, Polycom VBPs, and SBCs (Acme Packet Net-Net Enterprise Session Director) are not area-aware, which means they cannot be assigned to an area.
- Resources can belong to only one area, with the exception of DMA Pool Orders. If you want to share network devices between areas, you can leave them in no area.
- You can assign an area user an area role according to the tasks the user needs to perform in the RealPresence Resource Manager system. Area roles restrict user tasks to the area or areas in which they are allowed to manage.
- Some system-wide administration tasks cannot be delegated to users with only area-specific roles. These include site topology and conference templates. System maintenance and set up must also be done by a user with a system role.

Working within a Multi-Tenancy Environment

When using the RealPresence Resource Manager system's area feature, most aspects of the system become "area-aware" which means that management of the system and conferencing tasks may become different according to the role of the user.

The following aspects of the area feature are discussed in this topic:

- User Roles within a Multi-Tenancy Environment on page 429
- Area Address Books on page 431
- Area User Groups on page 431
- Area Users, Rooms and Associated Endpoints on page 431
- Area Conference Guests on page 432
- Using the Common Pool in a Multi-Tenancy Environment on page 432
- Area Conference Templates on page 432

User Roles within a Multi-Tenancy Environment

When you have enabled areas for your RealPresence Resource Manager system, you have access to additional user roles to help you delegate responsibilities to users within specific areas.

System Roles

System roles are used for users who are required to perform Resource Manager tasks for all areas. Resource Manager users that have a system role will be able to view and modify resources from all areas because their role includes the **View and/or Modify All Area**s permission.

System roles include: Administrator, Advanced Scheduler, Auditor, Device Administrator, Operator, Scheduler, and View-Only Scheduler.

For detailed information about system roles, see Working with Management Roles and Permissions on page 281.

Area Roles

An area role delegates Resource Manager responsibilities to a user that needs to manage the resources in one or more areas, but not all areas. A user must be assigned a RealPresence Resource Manager area role in order to perform his role-related tasks. In addition to being assigned a role, you must enable that user to manage the area(s) in which he needs to perform his responsibilities.

You can also allow a user to manage areas to which he does not belong. For example, you can allow an area scheduler to schedule users from two areas into conferences. For this, you would need to configure this user to manage both areas.

Area roles include: area administrator, area operator, and area scheduler.

Role	Permissions
Area Scheduler	Schedule Conferences Scheduling Level = Basic
Area Operator	Conference operator Reports Troubleshooting Schedule conferences, both basic and advanced. Schedule-able resource monitor. The area operator can monitor MCUs and DMA Pool orders that are in the areas he manages or in the common pool (no area).
Area Administrator	Add endpoints. Manage users and groups Monitor conferences Monitor network devices View-only scheduler Directory setup Can provision devices using existing profiles (cannot create provisioning profiles) Can update software on devices using existing software updates (cannot create software updates) Can add and edit users, groups, rooms, and other resources. Can view Reports for the area(s) they manage. No system-wide reports will be available. Can monitor the system via the Admin Dashboard. System-wide pods will not be available. Each sub-pod will have its source information filtered by area.

Area Conference Participants

Although conferences are area-specific, an area scheduler can add users from any area that he manages.

For example, if a area scheduler for the blue area was also granted permission to manage the yellow area, he can add conference participants from both the blue and yellow areas.

A system scheduler is able to schedule conferences in all areas and invite users from all areas.

Note that if a conference has participants, rooms, and/or guests from multiple areas, then Resource Manager users will be able to see the area names of only the areas that they belong to or can manage. Participants, rooms and guests that belong to other areas are presented as a “Guest of” the conference’s area.

Area Address Books

An address book must belong to only one area or to no area, but can contain users, endpoints, rooms and guests from multiple areas.

An address book is accessible to only users who are also assigned to the area that the address book belongs to. That is, if a user has a system role, they will see all address books, but if a user has only an area roles, they will see only address books that belong to the areas that they belong to or to areas in which they manage.

When a user views the contents of an address book that has members from multiple areas, they will be able to view only those members that belong to areas the user has access to. That is, if a user has a non-area-specific role, they will be able to see address book members from all areas, but if a user has only area-specific roles, they will see only members that belong to the areas they manage.

From an endpoint, an address book is accessible only if the logged in user and address book belong to the same area or if the logged in user manages the area the address book belongs to. When an endpoint user views the contents of a cross-area address book, the address book members they can see include:

- Members that belong to the same area as the user who is logged in to the endpoint
- Members that belong to other areas that the logged in user manages

Also note that changing the area that an address book is assigned to does not affect the areas of its members.

Area User Groups

User groups can be assigned to one area or no area. Although it can contain users from multiple areas. Users with the system role of administrator or the role of area administrator are allowed to create and edit user groups. If the area administrator manages more than one area, he can add users from any area that he manages to the user group. Remember that system administrators are automatically have permission to view/manage all areas, and can therefore add any user to a user group.

However, even if a group has users from multiple areas, area administrators can only view users within the group that belong to the areas they manage.

Changing the area of the group does not affect the area of the users in the group.

Area Users, Rooms and Associated Endpoints

Endpoints and rooms follow strict rules of staying in the same area of the user they are associated with. The Resource Manager system ensures that a user and their associated endpoint(s) belong to the same area. If one moves to another area or no area, the others move with it. The same is true for rooms and their associated endpoints. More specifically:

- If a user or room is put into an area or moved to a different area, all of their associated endpoints will be automatically updated to the same new area.
- If one of the associated endpoints of a user or room is moved to a different area, the change will propagate to the associated user or room and any other endpoints owned by the user or room.

The logged-in user is warned that this will happen so that they can cancel the operation if this is not what they intended. The only way to move an endpoint without also moving the owner and the owner's other endpoints is to disassociate the endpoint from the user or room before changing the area of the endpoint.

Area Conference Guests

When a new guest is added to a conference and saved to the guest book, the guest is configured to belong to the area that the conference belongs to. This area information of the guest is persisted in the guest book. If the conference's area changes after this point, the guest's area will not change. Users who can manage more than one area can change the guest's area by using the editing the guest book entry.

Using the Common Pool in a Multi-Tenancy Environment

If a network device or DMA pool order does not belong to an area, it is said to be in the "common pool" and therefore is available for the system to use for any area. Any user who manages an area and has permission to perform tasks within that area can view resources that are in the common pool.

For example, an area operator can schedule a conference on an RMX system that is explicitly assigned to the area to which the operator belongs or the scheduler can use an RMX system that belongs to the common pool.

Area Conference Templates

A user must have a system administrator role in order to create new conference templates. As a best practice, the same user responsible for system set up should be responsible for creating conference templates.

Conference templates can be assigned to an specific area and also associated with users with a specific role.

As a best practice, when you create a conference template, give it an area-specific name. This is especially helpful if you allow an area scheduler to scheduler conferences for more than one area.

When a scheduler (area or system) schedules a conference, he is required to use a conference template from the same area as the conference area or a template that is assigned to no area (common pool).

Configure Areas

You must configure your system for areas. Most of the configuration tasks can be completed by a user with the administrator role or area administrator role. However, network devices must be added by a user with the device administrator role.

You need to enable your system for areas and then add an area for each tenant that will use your system.

1 Enable the areas feature.

2 Add the areas that you want to use.

3 Customize the logos for each area, if desired.

4 Add network devices to areas. This task must be done by a user who has the device administrator role.

5 Import users into each area.

   This step is necessary if you need to support users who do not reside in your single LDAP directory. RealPresence Resource Manager system does not support integration with multiple LDAP directories.

6 Assign roles to area users. By default, area users all have the area scheduler role. You need to determine which, if any, of the area users will be given the area administrator or area operator roles.

7 Designate which users will manage each area.

   Users must be allowed to manage an area in order to perform the tasks associated with their area role. You can allow users to manage one area, no area, multiple areas (including areas to which they do not belong).

8 Add resources to areas. This task can be done by the Resource Manager system administrator, or a user with the area administrator who is also allowed to manage the area to which he is adding endpoints/rooms.

9 Add conference templates to areas. This task needs to be done by a user with the administrator role.

10 Configure site topology.

11 Add billing codes, if preferred.

Enable Areas

In order to enable areas for the RealPresence Resource Manager system, login to the system with a user who has the administrator role.

Users will need to log out and log back in to the RealPresence Resource Manager system in order for them to view any changes.

To enable the areas feature

1 Go to **Admin > Areas**.

2 From the list of Actions, select **Configure Areas.**

3 In the **Configure Areas** dialog box, ensure that the **Enable Areas functions in Resource Manager** box is checked.

4 Optionally, choose a name in which to refer to areas. For example, you can rename Area and Areas to Tenant and Tenants.

5 Click **Save Configuration**.

Create Areas for Tenants

For each new tenant, do the following:

1. Create a new area for the new tenant.
2. Give the area a name that appropriately identifies the tenant.
3. Create a user that will manage this area. You can do either of the following (or both).
   - Add at least one user to the tenant area who has the Area Administrator role and is set up to manage the area. That person can then manage their area themselves, including adding other users to manage the area and its resources.
   - You can also allow a user that belongs to no area or another area to manage the area and perform tasks, Assign Users to Manage an Area(s) on page 310.

Set up Area Management

The RealPresence Resource Manager allows you flexibility when setting up how to manage an area.

Manage the Area with System Roles

You can either have a set of users with system roles who manage the administrative and conference scheduling tasks for an area or you can set up area users with these roles and responsibilities.

In order for a user to perform tasks within ALL areas, a user must be given a system role that includes the View and/Or Modify all Areas permission. All system roles have this permission by default.

Manage the Area with Area Roles

In order for a user to perform tasks within a a single area, a user must be given the following:

- An area role
- Be configured to manage the area to which they need to perform their tasks.

  When associating a user with an area role, you must also explicit configure that user to manage the area. If the user is not allowed to manage the area, he cannot perform the tasks associated with his role. Area users can be configured to manage more than one area, see Assign Users to Manage an Area(s) on page 310.

Assign Resources to an Area

You need to assign resources to an area. Resources that belong exclusively to an area must be assigned to the area. Most resources can be created and assigned to an area by an Administrator or an Area Administrator.

Network devices must be assigned to an area by someone with the Device Administrator role.

Note about Conference Templates

The Administrator role is the only pre-defined role that can add or edit conference templates.

Can Belong to One or No Area

The following resources need to be assigned to one area or no area.

- Users
- Rooms
- Guests
- Groups
- Address Books
- Endpoints
- Network Devices
- Conferences
- Conference Templates
- Machine Accounts
- Peripherals

Can Belong to One or More Areas (or no Area)

Resources that can be associated with one or more areas or no areas are:

- DMA Pool Orders

Add Users to An Area

When you add users, create user names using the email address format. This will ensure that all user names are unique. Otherwise two people named Bob Smith belonging to different tenants may end up with the same user name. By following an email address format, Bob Smith in TenantA could have bsmith@tenantA.com as a user name and Bob Smith in TenantB could have bsmith@tenantB.com.

Configure Site Topology

You can use site topology to limit the bandwidth used by each tenant. This can be accomplished with a combination of a carefully organized site topology and the Site Statistics tool.

You can assign a site to a particular area. A site cannot be shared between areas.

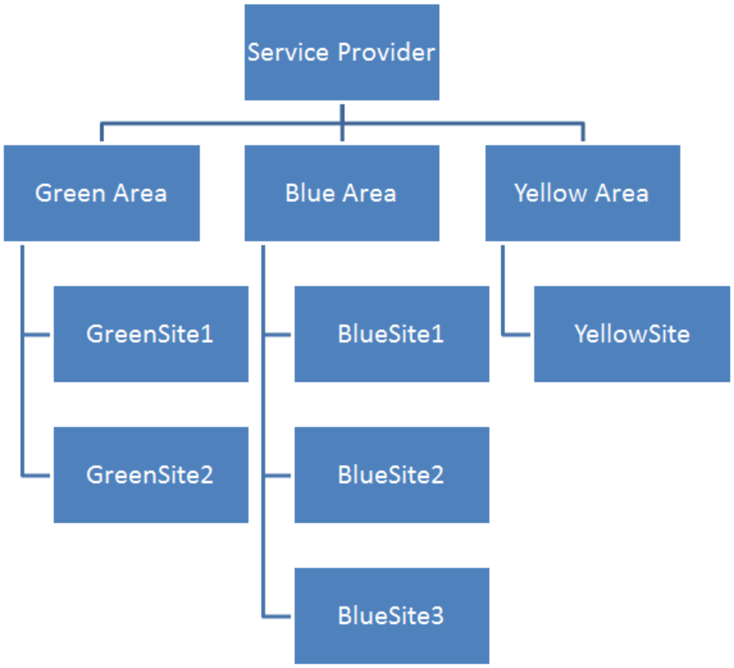
Use the following guidelines:

- As a best practice, use a naming convention that identifies the area in the site name. For example, all sites in the blue area should be named **blue_<sitename>**.
- Site names should be unique across the system. That is, two areas should not use the same site name.

- At a minimum, each site in an area should have a site link to the service provider or the internet cloud. It is best practice that the purpose of each link be obvious from the site link name. Any site link being used to measure bandwidth for a specific tenant should be named in such a way as to make this purpose clear.

Endpoints and devices should be associated with the same area to which their site belongs or they may not be visible to area constrained users when searching by site.

Figure: Site Topology for Multiple Tenants



Associating Billing Codes with Conferences

The RealPresence Resource Manager system supports associating a billing code with a conference. This feature is only available when areas are enabled.

You can define billing codes within an area that can then be assigned to conferences. When an area scheduler creates a conference within an area that includes billing codes, the scheduler can associate a billing code with that conference.

Billing codes are included in CDRs. This allows you to track how much each department (billing code) within an area is using video resources. Service providers can use this information to create billing breakdowns for their tenants.

Users with the Administrator role can create new billing codes for an area. Users with the area scheduler or area operator role are allowed to associate a billing code with a conference when the schedule the conference.

Adding a New Billing Code

Billing codes are supported when areas are enabled. You can add a billing code(s) to an area when you create an area or when you edit an existing area.

To add a new billing code

1 Navigate to **Admin > Areas.**

2 Click **Add** to add a new area.

OR

3 Select an area in the list and click **Edit**.

4 In the **Edit an Area** dialog box, click **Billing Code**.

5 On the **Billing Code** page, do the following:

   a In the **Billing Code** field, enter the billing code you want to use.

   b Enter a description for the billing code.

   c Click **Apply**.

6 Click **Ok**.

Note: To clear the billing code fields after an existing billing code in the list has been selected, click **Apply**.

Edit a Billing Code

You cannot modify an existing billing code. If you want to make any changes, delete the billing code and re-add it.

Deleting a Billing Code

Users with the administrator role can delete billing codes.

To delete a billing code

1 Navigate to **Admin > Areas**.

2 Select an area in the list and click **Edit**.

3 In the **Edit an Area** dialog box, click **Billing Code**.

4 On the **Billing Code** page, do the following:

   a Select a billing code.

   b Click Delete.

5 Click Ok.

Note: To clear the billing code fields after an existing billing code in the list has been selected, click **Apply**.

Associating a Billing Code with a Conference

When creating a new conference, you can select a billing code after you select conference participants.

Viewing Billing Code Information

The Conference Usage Report now includes billing code information for each conference. Billing code information is also include in conference information sent to the Polycom DMA system and the Polycom RMX systems.

When monitoring conferences, you can also filter conferences by billing code.

Managing Areas

This chapter describes how to manage areas in the Polycom® RealPresence® Resource Manager system. It includes these topics:

- View All Areas on page 439
- View Information for a Specific Area on page 439
- Customize the Area Logos (system and CMA Desktop) for the Area on page 442

View All Areas

You can view the list of existing areas from **Admin > Areas** if you have the Administrator role. The following information is available.

Field	Description
Name	Name for the area.
Description	Description of the area.
Area Resource Manager Users	Number of users that can manage the selected area.
Endpoints	Number of endpoints that belong to the selected area
Rooms	Number of rooms that belong to the selected area.
Members	Number of users that belong to the selected area.

View Information for a Specific Area

You can view all information for a specific area including resources and users.

You must be assigned the Administrator role to do this task.

To view information for a specific area

1. Go to **Admin > Areas**.
2. Click an area in the list.
3. The following **View** actions are available. The details you can view from each action is dependent on the type of resource it is. The following resources are available:

- **View Area Rooms**. For more information, see View the Rooms List on page 318.
- **View Area Resource Manager Users**. This action displays a list of all users who are allows to managed the selected area. For more information, see View User Information on page 290.
- **View Area Endpoints**. For more information, see View Endpoint Details on page 93.
- **View Area Guests**. For more information, see User Menu and Guest Book on page 312.
- **View Area Members**. This action provides a list of all users that belong to the selected area. For more information, see View User Information on page 290.
- **View Guests**. For more information, see Manage System Guest Book on page 311.
- **View Area Groups**. For more information, see Manage Groups on page 305.
- **View Area Address Books**. For more information, see Using Multiple Address Books on page 418.
- **View Area Conference**. For more information, see Managing Conferences and Participants on page 66.
- **View Direct Conference Templates**. For more information, see Direct Conference Templates on page 389.

Removing an Area

When you no longer need an area, you can either move the area's contents to another area or delete the area and all its contents. A user must have the Administrator role in order to move or delete an area.

Consider which of these approaches is right for the area:

If you wish to delete an area and all of its resources, then:

1. Backup your data.
2. Use the Delete action to delete the area and its resources.

If you wish to delete the area, but keep all of its resources in the Resource Manager system, then:

3. Use the Move Contents action to move all of the area's resources to another area or to no area. Move Contents will also delete the area from which contents are moved.

If you wish to keep some of the area's resources, but delete the rest, then:

4. Edit the resources you would like to keep and reassign them to other areas or to no area.
5. Backup your data.
6. Use the Delete action to delete the area and its remaining resources.

Moving the Contents of an Area

If you wish to delete the area, but keep all of its resources in the Resource Manager system, then you can move the contents of the area.

When you move the contents of an area:

- All resources will now belong to the specified destination (an area or no area).

- The area and any custom logos are deleted.
- Any users who managed the moved area will not be automatically allowed to manage the new area. If you want the moved users to manage the destination area, you will need to explicitly edit the user to do so.

Deleting an Area and its Resources

If you no long need an area and its resources, you can delete the area and its resources from the RealPresence Resource Manager system.

Before deleting an area, you must manually un-assign any network devices and sites from the area. You should also verify that there are no ongoing conferences or area users involved in a conference belonging to another area.

When you delete an area, the following actions take place:

- All future conferences are cancelled.
- All past conferences are associated with no area (None).
- All pool orders are disassociated from the area.

Users, rooms and endpoints from this area that have been participants, or are invited to be participants, in other areas' past or future conferences are disassociated from those conferences, such that:

- Resource Manager system conference reports for other areas will no longer include this area's participants.
- Future conferences for other areas will no longer include any participant from this deleted area. If a future conference is left with only one participant as a result, the conference will be canceled and the remaining participant will be notified.

If the previous action leaves any future conference in another area with only one participant, then the conference will be cancelled and the remaining participant will be notified by email.

If a conference template belonging to this area is referenced by a conference in another area, the template will be moved to no area. Otherwise the template is deleted.

All other resources in this area are deleted.

CDR data is not deleted or modified.

If an area is still in use when you try to delete it (a conference being scheduled, a resource being added), the area may not be completely deleted. If you receive an **Unable to Delete Area** message, it will detail resources that still need to be deleted. You will need to manually delete or re-assign these resources and then rerun the Delete Area action.

Before deleting an area, you must manually un-assign any network devices and sites from the area. You should also verify that there are no ongoing conferences or area users involved in a conference belonging to another area.

Disabling the Areas Feature

Disabling areas is not yet supported.

Customize the Area Logos (system and CMA Desktop) for the Area

You can customize the logos that a RealPresence Resource Manager system's area user sees when they log in to the RealPresence Resource Manager system or to their CMA Desktop client.

You must have the administrator role in order to customize logos. You can only customize logos for areas that you are allowed to manage.

Note

The RealPresence Resource Manager system must be running on an Internet Explorer browser or Google Chrome browser in order to upload a file.

To customize the system logo for an area

1 Go to **Admin > Area Logos**.

2 Click **Set Resource Manager System Logo**.

3 In the **Set Resource Manager System Logo** dialog box, browse to a file to upload and click **Upload**.

4 When the upload is complete, click **OK**.

To customize the CMA Desktop logo for CMA Desktop users within the area

1 Go to **Admin > Area Logos**.

2 Click **Set Resource Manager System Logo**.

3 In the **Set Resource Manager System Logo** dialog box, browse to a file to upload and click **Upload**.

4 When the upload is complete, click **OK**.

System Maintenance

This section provides an introduction to the Polycom® RealPresence® Resource Manager system maintenance. It includes:

- System Management and Maintenance
- System Redundancy
- Managing the Database
- System Reports
- Polycom RealPresence Resource Manager System SNMP
- Configuring Alert Settings
- System Backup and Recovery
- System Security and Port Usage

System Management and Maintenance

This chapter describes the following Polycom® RealPresence® Resource Manager system operations topics:

- Management and Maintenance Overview on page 444
- Recommended Regular Maintenance on page 445

Management and Maintenance Overview

The RealPresence Resource Manager system requires relatively little ongoing maintenance beyond monitoring the status of the system and downloading backups you want to archive. All system management and maintenance tasks can be performed in the management interface. See the appropriate topic for your user role:

- Administrator Responsibilities
- Auditor Responsibilities

Administrator Responsibilities

As a RealPresence Resource Manager system administrator, you're responsible for the installation, configuration, and ongoing maintenance of the system. You should be familiar with the following tasks and operations:

- Installing licenses when the system is first installed and when additional endpoints are added. See Server Settings on page 405.
- Monitoring system health and performing the recommended regular maintenance. See Recommended Regular Maintenance on page 445.
- Using the system tools provided to aid with system and network diagnostics, monitoring, and troubleshooting. See System Maintenance and Troubleshooting on page 489. Should the need arise, Polycom Global Services personnel may ask you to use these tools.
- Upgrading the system when upgrades/patches are made available. See Update the System Software on page 325.

Administrative Best Practices

The following are some of our recommendations for administrative best practices:

- Perform the recommended regular maintenance.

- Except in emergencies or when instructed to by Polycom Global Services personnel, don't reconfigure, install an upgrade, or restore a backup when there are active conferences on the system.
- Before you reconfigure, install an upgrade, or restore a backup, manually create a new backup of the system settings. You can then restore this backup in the event that something unforeseen occurs and it becomes necessary to restore the system to a known good state.
- For proper name resolution and smooth network operations, configure at least one DNS server in your network configuration, and preferably two or more. This allows the RealPresence Resource Manager system to function properly in the event of a single external DNS failure.
- Configure at least one NTP server in your time configuration and preferably two or more. Proper time management helps ensure that your system operates efficiently and helps in diagnosing any issues that may arise in the future. Proper system time is also essential for accurate audit and CDR data, as well as system redundancy.

Auditor Responsibilities

As a RealPresence Resource Manager system auditor, you're responsible for managing the system's logging and history retention. You should be familiar with the following configurations and operations:

- Configuring logging for the system. These settings affect the number and the contents of the log archives available for download from the system. Polycom Global Services personnel may ask you to adjust the logging configuration and/or download and send them logs.
- Configuring history retention levels for the system. These settings affect how much system activity history is retained on the system and available for download as CDRs.

Auditor Best Practices

The following are some of our recommendations for auditing best practices:

- Unless otherwise instructed by Polycom Global Services, configure system logging at the production level with a rolling frequency of every day and a retention period of 60 days. If hard drive space becomes an issue, decrease the retention period incrementally until the disk space issue is resolved.
- Download system log archives regularly and back them up securely (preferably offsite as well as onsite).
- Export CDRs regularly and back them up securely (preferably offsite as well as onsite).

For more information about managing audit logs, see Managing Audit Log Files on page 496.

Recommended Regular Maintenance

Perform the following tasks to keep your RealPresence Resource Manager system operating trouble-free and at peak efficiency. These tasks can be done quickly and should be run at least weekly.

Track System Alerts

You can track system alerts via email to remotely monitor the RealPresence Resource Manager system performance, see Configuring Alert Settings on page 476.

Create and Archive Backups

Log into the RealPresence Resource Manager system, go to **Admin > Backup System Settings** and **Create and Download a Backup Archive**. For more information, see Creating a System Backup Manually on page 486.

General System Health and Capacity Checks

On the **Dashboard** verify that there are no alerts indicating problems with any part of the system. For more information, see System Dashboard on page 360.

Certificates

Go to **Admin > Management and Security > Certificate Management** and verify that the list of certificates contains the certificates you've installed and looks as you would expect (an archived screen capture may be helpful for comparison).

Display the details for any certificate you've installed and verify they are as expected (an archived screen capture may be helpful for comparison). For more information, see Managing Security Certificates on page 346.

CDR export

If you want to preserve detailed call and conference history data in spreadsheet form off the RealPresence Resource Manager system, periodically download the system's CDR (call detail record) data to your PC.

System Redundancy

This chapter describes how to configure a redundant Polycom® RealPresence® Resource Manager system.

It includes these topics:

System Redundancy Overview

A redundant RealPresence Resource Manager system configuration offers higher reliability and greater call success by ensuring that a RealPresence Resource Manager system is always available.

A redundant RealPresence Resource Manager system configuration requires two RealPresence Resource Manager system servers and three IP addresses in the same subnet on the same network—one physical IP address for each of the servers and one virtual IP address dedicated to external access and endpoint registration.

This section includes the following topics:

How Redundancy Works

Terminology is very important in understanding how redundancy works.

In a redundant configuration, one server is licensed as the *primary server* and the other server is licensed as the *redundant server*. The primary server is always the primary server and the redundant server is always the redundant server.

In a redundant configuration, there is only one *active server* and only one *inactive server*. The active server is the server currently managing endpoints and monitoring conferences. It is actively responding to network traffic routed to the virtual IP address. In a normal operational state, the active server is the primary server. In a failover state, the active server is the redundant server.

The active/inactive servers communicate over a dedicated private network using a LAN cable physically connected from one server to the other. The active/inactive servers communicate every 1000 milliseconds using a private IP address and port 5405. If the inactive server does not receive 4 consecutive heartbeats (i,e, four seconds) from the active server, it will promote itself to being the active server.

The most common reasons for system failovers are power failures and network disconnections. Failures in services running on the primary server also initiate a failover.

If both the primary and redundant servers start simultaneously (for example if both are in the same location and recover from a power failure at the same time), both servers will initially attempt to become the active server. Whichever server starts first becomes the active server.

An administrator can force a failover via the **Switch Server Role** function in the RealPresence Resource Manager system user interface.

Also, the failover to the redundant server occurs seamlessly because the endpoints are registered with the virtual IP address, which remains constant. However, endpoints that are dynamically managed will lose the connection as the provisioning service will stop for approximately five minutes.

During a failover:

- Users logged into the RealPresence Resource Manager system user interface are disconnected during a failover and returned to the main RealPresence Resource Manager system web page. Users can log back in once the 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.
- The redundant server becomes the active server. Its services start in an order designed to prevent the new active server from being flooded with requests from endpoints during startup.

A system failover usually takes approximately 5 minutes.

Once a failover to a redundant server occurs, the redundant server manages all system operations until another failover occurs or if administrator switches back to the original primary server via the **Switch Server Roles** function in the RealPresence Resource Manager system user interface.

Notes

- The RealPresence Resource Manager system does not automatically switch to the primary server when the primary server becomes available. An administrator may **Switch Server Roles** if needed.

Redundant Configuration System Administration

The system database is replicated between the two servers so most of their configuration information is shared. In order for the system database to be synchronized accurately, basic network settings for the two servers must match.

The following settings must match between the two servers and be configured before setting up redundancy.

This includes:

- Basic network settings such as IP, default gateway, and DNS settings

- Time and external NTP server settings

Warning

You cannot execute manual commands while redundancy is configured.

Licensing

Licensing and upgrading a redundant system is slightly more complex. The primary and redundant servers require different licenses.

Data Loss

Under some circumstances, data loss cannot be avoided. If one server has been down for quite some time, its data may be out of date. If the system fails over while out of sync, database data may be lost.

Considerations for Redundancy

Consider the following:

1. During first-time set up for each server, use the same NTP server for both servers. You cannot modify the NTP server settings after setting up redundancy.
2. Ensure each system uses the same RealPresence Resource Manager software version.
3. You **MUST** set up redundancy before uploading any licenses.
4. Ensure both systems are up and running before configuring redundancy.
5. If configuring redundancy on an existing system, Polycom recommends making a system backup before configuring redundancy.
6. When adding redundancy to an existing system, be sure to set up redundancy on the existing server first. If you set up redundancy in the wrong order, data will be lost.
7. You cannot change the system name or domain name after configuring redundancy.

Implement a Redundant System

A redundant system configuration requires the installation of two RealPresence Resource Manager system servers on the same network. During **First Time Setup**, you are instructed to assign these two servers physical IP addresses.

These topics describe how to complete the configuration of these newly installed redundant servers. It includes these topics:

- Perform a System Backup on page 450
- Perform Network Configuration on Both Servers on page 450
- Connect the Servers to Each other Via Cable on page 450
- Ensure You Have Appropriate Licenses for Both Servers on page 450
- Configure the Both Servers for Redundancy on page 450

- License a Redundant System on page 451

Perform a System Backup

If you are setting up redundancy for an existing RealPresence Resource Manager that has already been active, you should first backup your existing system. See Creating a System Backup Manually on page 486.

Perform Network Configuration on Both Servers

Install both of your RealPresence Resource Manager systems as described in the *Polycom Resource Manager Getting Started Guide*.

- Be sure they are both configured to the same NTP server.
- Be sure that all RealPresence Resource Manager passwords are the same on both systems before configuring redundancy.

Connect the Servers to Each other Via Cable

Polycom recommends directly connecting the servers to each other using a **crossover** cable if there is no need for geo-redundancy. Place the connecting cable on the second network port.

Redundancy with Servers in Disparate Locations

Polycom supports having the two RealPresence Resource Manager systems in different geographic locations if the following conditions are met:

- Network latency less than 100 ms
- Dedicated VLAN for the 1 to 2 communication (to emulate the cross-over cable)
- Network switch must support multicast packets.
- Same client side IP space must be used in both data centers. For example, one domain controller A has a physical server A with its IP, and domain controller B has a physical server B with its IP and the virtual IP is still shared between the domain controllers.

Ensure You Have Appropriate Licenses for Both Servers

Follow the steps on Request a Software License File on page 342.

Configure the Both Servers for Redundancy

You need to configure both servers for redundancy.

To set up redundancy for your environment

1. On the server, go to **Admin > Server Settings > Redundant Configuration**.
2. Enter the **IP Settings** for the redundant system and click **Submit**.

IP Setting	Definition
Virtual IP	This virtual IP address of the redundant server. You only need to configure a value for the Virtual IP address on the primary server where the primary license will be installed.
Virtual Host Name	The hostname that corresponds to the virtual IP address.
Local Server IP	This is the IP address of the local server. It is read automatically and is readonly.
Peer Server IP	The IP address of the second server in your configuration.

The primary system will reboot.

3 Verify that you can access the primary server.

4 Repeat these steps on the redundant (second) server.

License a Redundant System

This topic describes how to license a redundant system. You will need a primary license for one server and a secondary license for the second server.

You need to update both license files by accessing the RealPresence Resource Manager system using the virtual IP address.

To license a non-redundant Resource Manager system, see Add System Licenses on page 341.

To license a redundant system

1 Request a both a primary license for the primary server and a secondary license for the secondary server as described in Request a Software License File on page 342.

2 Log into the RealPresence Resource Manager system *using the virtual IP address*, and go to **Admin > Server Settings > Licenses**.

3 Click **Update License**.

4 Follow the instructions on the **Update License** dialog and be sure you have a backup copy of your initial license file.

5 Click **Choose File** and navigate to the primary license file you requested.

6 Click **Preview** and then click **Apply**.

7 Click **Update License** again.

8 Follow the instructions on the **Update License** dialog

9 Click **Choose File** and navigate to the secondary license file you requested. Then click **Apply** after **Preview** correctly.

Managing a Redundant System

After you have configured your system for redundancy, you can track system failovers and manually initiate a system failover.

This section includes the following topics:

- Manually Failover to a Redundant Server on page 452
- Track System Failovers on page 452
- Discontinue Redundancy on page 453

Manually Failover to a Redundant Server

In a redundant configuration, the system automatically fails over from the primary server to the redundant server. However, you can also manually initiate a failover.

> The Switch Server Role option is not available if the inactive server is not available.

To manually initiate a failover

1 On either server, go to **Admin > Server Settings > Redundant Configuration**.

2 On the **Redundant Configuration** page, click **Switch Server Role**.

The system initiates a failover to the other server.

Track System Failovers

You can monitor how and when the system has failed over. The RealPresence Resource Manager system provides detailed messages about the time and reason for a system failover.

You can also view system failover information in the System Alerts pane and on the System Dashboard (Redundancy pane).

To view the time and reason of the last system failover

1 Navigate to **Admin > Server Settings > Redundancy**.

2 View the read-only information for the time and reason of the failover.

Failover Reason	Definition
Public NIC is down.	The network interface card went down on the active server.
Gateway is unreachable.	The active system could not reach the network gateway either because the network cable is unplugged or for network issues external to the system.
Web application is down.	The application service on the active server stopped and the web interface cannot be reached.

Failover Reason	Definition
Database is down.	The system database went down on the active server.
Site topology database is down.	The site topology database went down on the active server (Opends database).
Manual failover.	The failover was manually initiated by the administrator.
Active server not responding.	The active server could not be reached.

Discontinue Redundancy

In some circumstances, you may need to discontinue redundancy.

To discontinue a redundant configuration when the system is in a valid redundant state

Use this procedure to discontinue redundancy, but only when the system is in a valid redundant state.

1. Log into the system *using the virtual IP address*.
2. Go to **Admin > Server Settings > Redundant Configuration**.
3. On the **Redundant Configuration** page, click **Reset Redundant Configuration**.

   The two servers restart as single server.

To discontinue a redundant configuration if only one server can be accessed

If only one server can be accessed, discontinue redundancy on that server first. Discontinue redundancy on the other server after it can be accessed.

1. Log into the system *using the virtual IP address*.
2. Go to **Admin > Server Settings > Redundant Configuration**.
3. On the **Redundant Configuration** page, click **Reset Redundant Configuration**.

   The primary system restarts as single server.
4. When the redundancy server can be accessed (Now it promotes to active server), log into the system *using the virtual IP address*.
5. Go to **Admin > Server Settings > Redundant Configuration**.
6. On the **Redundant Configuration** page, click **Reset Redundant Configuration**.

   The system restarts as single server.

Managing the Database

This chapter describes the Polycom® RealPresence® Resource Manager database integration and operations. It includes these topics:

Overview of the RealPresence Resource Manager System Database

The RealPresence Resource Manager system automatically optimizes its internal database on an ongoing basis. Database backup files are created when you run system backups, see Creating a System Backup Manually on page 486.

Database Restoration

You can restore the database by performing a system restoration, see Restore from a Backup Archive on page 488.

Reformat the Existing Database

The RealPresence Resource Manager system has an option that allows you to completely reformat (clean out) the system's existing database.

> Use this option only if your database is corrupted beyond repair or perhaps if you need to wipe out a test system to prepare it for production data.

To reformat the existing database

1 From the RealPresence Resource Manager system web interface, go to **Admin > Server Settings > Database**.

2 On the **Database** page, select **Reformat existing database...**

3 Click **Yes** to confirm the reformat operation.

The system displays a **Reformat/Install Progress** bar to indicate that the system is reformatting the database.

System Reports

This chapter describes the reports available through the Polycom® RealPresence® Resource Manager system and how to view and export them. Use these reports to identify return on investment, troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls. It includes these topics:

- Report Considerations for Multi-Tenancy on page 456
- Site Statistics Report on page 456
- Site Link Statistics Report on page 457
- Endpoint Usage Report on page 459
- Conference Usage Report on page 464
- Conference Type Report on page 465

Report Considerations for Multi-Tenancy

Area-specific information displays in reports when you have either the administrator role or the area administrator role AND can manage more than one area.

Site Statistics Report

Use the **Site Statistics** report to check call rate and call quality statistics for the sites. You can view the data in a grid or graphically.

To view Site Statistics

1 Go to **Reports > Site Statistics**.

The **Site Statistics** appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds.

Column	Description
Site Name	Specifies the site to which the statistics apply.
Num of Calls	Specifies the number of currently active calls for the site.
% Bandwidth Used	Specifies the cumulative bandwidth used by the currently active calls.

Column	Description
Bandwidth	
Avg Bit Rate	Specifies the average bit rate for the currently active calls that is, the total bit rate for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Avg Jitter	Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.
Avg Delay	Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.

2 To view the **Site Statistics** graphically and over a selected period of time:

a Click **View Chart**.

b In the **Site Name** list, select the site(s) to chart.

c In the **Y-Axis** list, select the statistic(s) to chart.

d In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

The charts are dynamically updated for your selections.

Site Link Statistics Report

Use the **Site Link Statistics** report to check call rate and call quality statistics for all site links. You can view the data in a grid or graphically.

To view Site Link Statistics

1 Go to **Reports > Site Link Statistics**.

The **Site Link Statistics** appear with the statistics displayed in a grid. The grid shows a snapshot of the current statistics. The data is updated automatically every 15 seconds.

Column	Description
Site Link Name	Specifies the two linked sites for which the statistics apply.
Num of Calls	Specifies the number of currently active calls for the site link.
% Bandwidth Used	Specifies the percentage of bandwidth used by the currently active calls, that is, the bandwidth used by the currently active calls divided by the total available bandwidth for the link expressed as a percentage.
Bandwidth	Specifies the total bandwidth of the link.

Column	Description
Avg Bit Rate	Specifies the average bit rate for the currently active calls, that is, the total bit rate for all currently active calls divided by the number of active calls.
% Packet Loss	Specifies the average percentage of packet loss for the currently active calls that is, the total percentage of packet loss for all currently active calls divided by the number of active calls.
Avg Jitter	Specifies the average jitter for the currently active calls that is, the total jitter for all currently active calls divided by the number of active calls.
Avg Delay	Specifies the average delay for the currently active calls that is, the total delay for all currently active calls divided by the number of active calls.

2 To view the **Site Link Statistics** graphically:

   a Click **View Chart**.

   b In the **Site Name** list, select the site(s) to chart.

   c In the **Y-Axis** list, select the statistic(s) to chart.

   d In the **Data Limit** field, enter the time frame in minutes for which to chart the data. The default is 60 minutes.

   The charts are dynamically updated for your selections. The site-links are displayed in the same order as the site-link grid.

Call Detail Record Report Administration

By default, the RealPresence Resource Manager system stores the conference and endpoint call detail records (CDRs) for 30 days. You can modify the CDR retention period and you can schedule a weekly archive of the CDRs. These procedures are described in the following topics.

Modify the CDR Retention Period

By default, the conference and endpoint CDRs are purged after 30 days.

To change how long CDR information is retained

1 Go to **Reports > Report Administration**.

2 In the **Report Administration** page, enter the number of days for the **Retention Period for Conference and Endpoint CDRs**.

3 Click **Save Settings**.

Schedule Archives of the CDR Report

You can schedule archives of CRD reports to be sent to an external server for storage.

To schedule archives of CDR information

1. Go to **Reports > Report Administration**.
2. In the **Report Administration** page, select **Enable FTP of CDR Records (CSV Format)**.
3. Configure these settings:

Field	Description
Next Transfer Date	Set the date for the next CDR transfer.
Transfer Start Time	Set the start time of the next transfer and all subsequent transfers.
CDR Transmission Frequency (In Days)	Set the number of days between each transfer.
Host name or IP Address of FTP server	Specifies the server to which the archives will be transferred. By default, the system transfers the archives to a location on its local server. You can change this to an external server.
FTP Port	Specifies the port through which the archives will be transferred. By default, this is system port 21.
FTP User Name/ FTP Password/ Confirm FTP Password	Specifies a user name and password combination for accessing the FTP server. This must be a valid user account on the FTP server.
FTP Directory	Specifies the directory on the server to which the archives will be transferred.

4. To verify that the FTP settings are functional, click **Test Archive Settings**.
5. When the settings are correct, click **Save Settings**.

Endpoint Usage Report

The **Endpoint Usage Report** is based on the CDRs extracted from selected endpoints and includes entries for ISDN and IP calls.

Currently, the RealPresence Resource Manager system reports CDRs for the following endpoints:

- Polycom HDX Series
- Polycom VVX
- CMA Desktop
- RealPresence Group series
- RealPresence Immersive Studio systems.
- Supported Cisco and LifeSize endpoint models

Use data from the **Endpoint Usage Report** to troubleshoot problems, provide information about network traffic, and ensure accurate billing for Polycom video calls.

To view the Endpoint Usage Report

1 Go to **Reports > Endpoint Usage Report**.

The **Endpoint Usage Report** page appears displaying the following information for the endpoints for which CDRs are available.

Field	Description
Serial Number	The registered serial number of the endpoint.
Endpoint Name	The registered name of the endpoint.
Site	The location at which the endpoint resides. **Note** When areas are enabled on your system, this field shows a value of **Restricted** if you do not have permission to manage the area to which the site is assigned.
Owner/Room	The person or room to whom the endpoint is registered.
Area	Displays the area to which the endpoint is associated. This column only available when areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage. If you do not have permission to manage the area in which the endpoint belongs, the value in this column reads, “Restricted”.

The CDRs are displayed in alphabetical order for the default **Start Date** and **End Date**. By default, the CDRs for the last week are reported.

2 To restrict the report to a different time period, change the **Start Date** and **End Date**. The report is dynamically updated.

3 Use the **Filter** to customize the report by endpoint **Type**, **Name**, **IP Address**, **ISDN Video Number**, **Alias**, **Site**, or **VIP** status.

You can also filter on **Area** when areas are enabled and you manage more than one area.

4 To generate the Endpoint Usage report, select one or more endpoints to include in the report and click **Generate Report**. Use the CTRL key, to select multiple endpoints.

The **Generate Report** page displays the **Summary** usage report for the selected endpoints. It includes the following information for the calls.

Field	Description
Number of calls	Specifies the number of calls the selected endpoints joined for the selected date range. Click **Details** to get more information about these calls.
Total call time	Specifies the total amount of time the selected endpoints spent in conference during the selected date range.

Field	Description
Average time per call	Specifies the average amount of time the selected endpoints spent in conference during the selected date range, that is, the total call time divided by the number of calls.
Average rate per call	Specifies the average bit rate for the selected calls.

5 To select a different group of endpoints, click **Change Selected**, select the endpoints, and click **Generate Report** again.

6 Click **Call Times** to see a chart that identifies the number of calls versus the start time for the calls.

7 Click **Inbound** to see a chart that identifies the endpoints from which the inbound calls to the selected endpoints originated.

8 Click **Outbound** to see a chart that identifies the endpoints to which the selected endpoints called.

9 Click **Summary CDR Report** to see a grid that displays information for each of the selected endpoints that participated in calls.

Field	Description
Serial Number	The registered serial number of the endpoint.
Endpoint Name	Identifies the endpoint by name.
Total Time in Call	Specifies the total amount of time the endpoint spent in conference during the selected time period.
Average Time in Call	Specifies the average amount of time the endpoint spent per call during the selected time period, that is, the **Total Time in Call** divided by the **Total Calls**.
Average Speed All Calls	Specifies the average bit rate for all of the calls in which the endpoint participated during the selected time period, that is, total bit rate divided by the **Total Calls**.
Calls Out	Specifies the number of calls in which the endpoint participated during the selected time period that originated from the endpoint.
Calls In	Specifies the number of calls in which the endpoint participated during the selected time period that did not originate from the endpoint.
Total Calls	Specifies the total number of calls in which the endpoint participated for the selected time period.

If any of the selected endpoints did not participate in calls during the selected time period, it is not included in the **Summary CDR Report**.

10 To export the information in the **Summary CDR Report**, click **Export as Excel File** and either **Open** or **Save** the file as needed. Note that only the first 1000 lines of the report are exported to the Excel file.

11 Click **Detail CDR Report** to see information for each of the endpoints that participated in calls.

The **Generate Report** page displays **System Information** and CDR information for the first endpoint in the list. For the selected endpoint, the **System Information** section includes the following data.

Field	Description
System Information	Specifies the name of the selected endpoint.
Area	The area to which the endpoint is assigned. This field is only visible when Areas are enabled. A user can only view area-specific information for an area(s) that he has permission to manage.
Model	Specifies the model number of the selected endpoint.
IP Address	Specifies the IP address of the selected endpoint.
ISDN	Specifies the ISDN number or V.35 number.
Serial Number	Specifies the serial number of the selected endpoint.

For each call from the selected endpoint, the CDR information includes the following data.

Field	Description
Start Date Time	Specifies the start date and time for the conference.
End Date Time	Specifies the end date for the report. This also defaults to the current date.
Call Duration	Specifies how long the call lasted in hours, minutes, and seconds.
Account Number	If Require Account Number to Dial is enabled on the system, the value entered by the user is displayed in this field.
Remote System Name	Specifies the endpoint to which the endpoint was connected for the call.
Call Number 1 Call Number 2	Specifies the IP or ISDN numbers for the endpoints to which the endpoint was connected for the call.
Transport Type	The type of call — Either H.320 (ISDN), H.323 (IP), or SIP.
Call Rate	The bandwidth negotiated with the far site.
System Manufacturer	The name of the system manufacturer, model, and software version, if they can be determined.
Call Direction	In — For calls received. Out — For calls placed from the system.
Conference ID	A number given to each conference. A conference can include more than one far site, so there may be more than one row with the same conference ID.
Call ID	Identifies individual calls within the same conference.
H.320 Channels	The total number of ISDN B channels used in the call. For example, a 384K call would use six B channels.
Endpoint Alias	The alias of the far site.

Field	Description
Endpoint Additional Alias	An additional alias of the far site.
Endpoint Type	Terminal, gateway, or MCU.
Endpoint Transport Address	The actual address of the far site (not necessarily the address dialed).
Audio Protocol Tx	The audio protocol transmitted to the far site, such as G.728 or G.722.1.
Audio Protocol Rx	The audio protocol received from the far site, such as G.728 or G.722.
Video Protocol Tx	The video protocol transmitted to the far site, such as H.263 or H.264.
Video Protocol Rx	The video protocol received from the far site, such as H.261 or H.263.
Video Format Tx	The video format transmitted to the far site, such as CIF or SIF.
Video Format Rx	The video format received from the far site, such as CIF or SIF.
Disconnect Info	The description of the Q.850 (ISDN) cause code showing how the call ended.
Q850 Cause Code	The Q.850 cause code showing how the call ended.
Total H.320 Errors	The number of errors during an H.320 call.
Avg % Packet Loss Tx	The combined average of the percentage of both audio and video packets transmitted that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.
Avg % Packet Loss Rx	The combined average of the percentage of both audio and video packets received that were lost during the 5 seconds preceding the moment at which a sample was taken. This value does not report a cumulative average for the entire H.323 call. However, it does report an average of the sampled values.
Avg Packet Loss Tx	The number of packets transmitted that were lost during an H.323 call.
Avg Packet Loss Rx	The number of packets from the far site that were lost during an H.323 call.
Avg Latency Tx	The average latency of packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Avg Latency Rx	The average latency of packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Max Latency Tx	The maximum latency for packets transmitted during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Max Latency Rx	The maximum latency for packets received during an H.323 call based on round-trip delay, calculated from sample tests done once per minute.
Avg Jitter Tx	The average jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.

Field	Description
Avg Jitter Rx	The average jitter of packets received during an H.323 call, calculated from sample tests done once per minute.
Max Jitter Tx	The maximum jitter of packets transmitted during an H.323 call, calculated from sample tests done once per minute.
Max Jitter Rx	The maximum jitter of packets received during an H.323 call, calculated from sample tests done once per minute.

12 To export the information, click **Download Report** and either **Open** or **Save** the CDR report in Microsoft Excel format for the selected endpoint or in CSV format **For All Selected Endpoints**. Note that only the first 1000 lines of the report are exported to the Excel file.

13 Click **Change Selection** to return to the **Endpoint Usage Report** page to select a different endpoint.

Conference Usage Report

Use the **Conference Usage Report** option to review usage information about system conferences.

To create a Conference Usage Report:

1 Go to **Reports > Conference Usage Report**.

An empty **Conference Usage Report** grid displays.

2 As needed, change the **Start:** and **End:** dates to select the date range for the report.

Select Summary Report or Detail Report. These reports includes the following:

Field	Description
Conference Name	Name of the conference.
Conference Scheduler	Name of the user who scheduled the conference.
Conference Scheduler ID	ID of the user who scheduled the conference.
Date	Date of the conference.
Scheduled Start	Scheduled start time of the conference.
Scheduled Stop	Scheduled stop time of the conference.
Scheduled Duration	Scheduled duration of the conference.
Actual Start	The actual time the conference started.
Actual Stop	The actual time the conference stopped.
Actual Duration	The actual duration of the conference. If the duration of the conference is less than sixty seconds, the conference duration is displayed as zero.

Field	Description
Total Scheduled Participants	Total number of scheduled participants for the conference.
Total Actual Participants	Total number of actual participants who attended the conference.
Billing Code	Billing code is listed if areas are enabled and a billing code was assigned to the conference. If areas are enabled and a billing code is not assigned, the value is None.

Conference Type Report

Use the **Conference Type Report** option to review monthly summary information about past RealPresence Resource Manager system conferences.

To create a Conference Type Report

1 Go to **Reports > Conference Type Report**.

An empty **Conference Type Report** grid appears.

2 If areas are enabled and you manage more than one area, you can use the **Belongs To Area** drop-down list to filter the conference types by area.

3 As needed, change the **From:** and **To:** dates to select the date range for the report, and click **View**.

The **Conference Type Report** for the selected date range appears. It includes the following information.

Column	Description
Date	Information is displayed on a month-by-month basis and an average for the selected months.
Area	This field is only visible when Areas are enabled. You can only view area-specific information for area(s) that you have permission to manage.
Scheduled	The number of conferences scheduled with the RealPresence Resource Manager system scheduling interface.
Ad hoc	The number of conferences that used one or more endpoints that are registered to the RealPresence Resource Manager system, but that weren’t scheduled via the RealPresence Resource Manager system scheduling interface. Ad hoc conference information can only be viewed by users with the administrator role. Although users with area administrator roles who manage more than area can view this column, the value will always be zero because ad hoc conferences are not associated with areas. Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager system. Monitoring information will be incorrect and inconsistent.

Column	Description
Multipoint	The number of multipoint conferences scheduled using the RealPresence Resource Manager system scheduling interface.
Point-to-Point	The number of point-to-point conferences scheduled using one of the RealPresence Resource Manager system scheduling interfaces.
Gateway	The number of scheduled conferences that used a gateway to reach one or more endpoints.
Embedded Multipoint	The number of scheduled multipoint conferences that used the MCU embedded in a V-Series, VSX-Series, or Polycom HDX-Series endpoint rather than an external MCU such as an RMX MCU.
Two Person Conferences on MCU	The number of scheduled point-to-point conferences that used an external MCU such as an RMX MCU even through point-to-point conferences do not usually require MCU resources.
Short	The number of scheduled conferences that were scheduled to last 30 minutes or more, but which actually lasted less than 30 minutes.
Scheduled Minutes	The sum of the scheduled minutes for all RealPresence Resource Manager system scheduled conferences.
Executed Minutes	The sum of the actual minutes for all RealPresence Resource Manager system scheduled conferences.
Total Participants	The sum of the participants that joined RealPresence Resource Manager system scheduled conferences.
Avg Participants in Multipoint	The average number of participants that joined scheduled RealPresence Resource Manager system multipoint conferences.

4 To create one of the conference type report charts, click the appropriate chart name below the grid. Chart choices include:

Column	Description
Scheduled vs. Ad hoc	A chart that compares the number of scheduled conferences to the number of ad hoc conferences. Ad hoc conference information can only be viewed by users with the administrator role. Although users with area administrator roles who manage more than area can view this column, the value will always be zero because ad hoc conferences are not associated with areas. Ad hoc conferences that take place on MCUs that are managed by the Polycom DMA system cannot be monitored by the RealPresence Resource Manager system. Monitoring information will be incorrect and inconsistent.
Scheduled	A chart that compares the number of point-to-point, multipoint, gateway, and embedded multipoint conferences.
Scheduled vs. Executed Mins	A chart that compares the number of scheduled minutes to the number executed minutes.
Avg Participants in Multipoint	A chart that displays the average number of participants in multipoint conferences.
Two Person on MCUs	A chart that displays the number of point-to-point conferences hosted on an external MCU.

The selected chart dynamically appears below the grid.

5 To export the report:

a Click **Export**.

b In the **File Download** dialog box, click **Save**.

Polycom RealPresence Resource Manager System SNMP

This chapter provides a discussion of the Polycom® RealPresence® Resource Manager system SNMP support. It includes these topics:

SNMP Overview

Simple Network Management Protocol (SNMP) is a IP-based communication protocol that allows network management systems to manage resources across a network.

SNMP communication takes place between the management system and SNMP agents, which are the hardware and software that the management system monitors. An agent collects and stores local system information and makes this information available to the management system via SNMP.

The RealPresence Resource Manager system includes an SNMP agent. It translates local system information into the format defined by the MIB.

The RealPresence Resource Manager system resides on a Polycom-branded Dell server. The Dell server software also includes an SNMP agent and MIB (Message Information Base). However, the RealPresence Resource Manager system acts as a proxy agent to forward the Dell server MIB alarms and alerts, so the management system does not need to be configured to receive information directly from the Dell server MIB.

Polycom recommends using a MIB browser to explore the RealPresence Resource Manager system MIB. The RealPresence Resource Manager system MIB is self-documenting and includes information about the purpose of specific traps and inform notifications.

It is important to note that you should understand how your SNMP management system is configured to properly configure the RealPresence Resource Manager system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements on the RealPresence Resource Manager system.

The RealPresence Resource Manager system supports three SNMP levels:

- **Disabled**—The RealPresence Resource Manager system SNMP processes are turned off.
- **SNMPv2c**—The RealPresence Resource Manager system implements a sub-version of SNMPv2. The key advantage of SNMPv2c is the Inform command. Unlike Traps, Informs are messages sent to the management system that must be positively acknowledged with a response message. If the management system does not reply to an Inform, the RealPresence Resource Manager system resends the Inform. SNMPv2c also has improved error handling and improved SET commands.

  One drawback of SNMPv2c is that it is subject to packet sniffing of the clear text community string from the network traffic, because it does not encrypt communications between the management system and SNMP agents.

- **SNMPv3**—The RealPresence Resource Manager system implements the newest version of SNMP. Its primary feature is enhanced security. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity. The `contextEngineID` is used to generate the key for authenticated messages.

  The RealPresence Resource Manager system implements SNMPv3 communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB).

  - Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.
  - Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.

SNMP v3 Users

- When upgrading to v8.1, you will need to modify the SNMP agent settings on your MIB browser in order to keep receiving SNMP information. You need to clear the “context name” from the agent settings. It is no longer used.

Working with SNMP

RealPresence Resource Manager system uses SNMP to provide a standardized framework and a common language used monitoring and managing the system.

The RealPresence Resource Manager system incorporates the common Polycom management framework data model. This includes system-specific SNMP MIBs, support for receiving hardware traps from both servers in a redundant system, and an SNMP rest API.

Polycom provides several MIB files that contain specific to RealPresence Resource Manager operations as well as MIBs that track hardware operations. Hardware MIBs such as CPU temperature and so on are tracked using Dell-specific MIBs made available from the RealPresence Resource Manager system.

You can configure what version of SNMP to use as well as set up notification receivers to help you track RealPresence Resource Manager system activities.

This section describesthe system SNMP operations including:

- Enable SNMP Messaging on page 469
- Download RealPresence Resource Manager System MIB Package on page 474

Enable SNMP Messaging

To enable SNMP messaging you must perform the two tasks:

1. Edit the SNMP Settings for a RealPresence Resource Manager System on page 469
2. Add an SNMP Notification Receiver on page 471

Edit the SNMP Settings for a RealPresence Resource Manager System

You can configure the system SNMP settings.

To edit the SNMP settings for a RealPresence Resource Manager system

1. Go to **Admin > SNMP Settings**.
2. To enable SNMP, select an **SNMP Version**. For information on the SNMP versions, see SNMP Overview on page 468.

3 Configure these settings for the connection between the RealPresence Resource Manager system and the SNMP agents on the **SNMP Setting** page.

Setting	Description
Transport	Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocol: **TCP**—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP. **UDP**—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent. Because UDP doesn't have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring.
Port	Specifies the port that the RealPresence Resource Manager system uses for general SNMP messages. By default, the RealPresence Resource Manager system uses port 161.
Community	For SNMPv2c, specifies the context for the information, which is the SNMP group to which the devices and management stations running SNMP belong. The RealPresence Resource Manager system has only one valid context—by default, `public`—which is identified by this **Community** name. The RealPresence Resource Manager system will not respond to requests from management systems that do not belong to its community.
Supported MIB	You can select from a list of RealPresence Resource Manager-specific MIBs to maintain. The MIB you select determines the which TRAPs are sent to the TRAP receivers you set. GET operations are supported for both MIBs. • POLYCOM_RESOURCE_SCHEDULER_MANAGEMENT • POLYCOM_CMA_MIB (legacy MIB)
V3 Local Engine Id	For SNMPv3, displays the RealPresence Resource Manager system `contextEngineID` for SNMPv3.
Security User	For SNMPv3, specifies the security name required to access a monitored MIB object. This name cannot be snmpuser.
Auth Type	For SNMPv3, specifies the authentication protocol. These protocols are used to create unique fixed-sized message digests of a variable length message. The RealPresence Resource Manager system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB). Possible values for authentication protocol are: • MD5—Creates a digest of 128 bits (16 bytes). • SHA—Creates a digest of 160 bits (20 bytes). Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet.

Setting	Description
Auth Password	For SNMPv3, specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.
Encryption Type	For SNMPv3, specifies the privacy protocol for the connection between the RealPresence Resource Manager system and the SNMP agent. The RealPresence Resource Manager system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB). Possible values for privacy protocol are: • DES—Uses a 56 bit key with a 56 bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128 bit key with a 128 bit salt to encrypt the SNMPv3 packet.
Encryption Password	For SNMPv3, specifies the password to be associated with the privacy protocol.

4 Click **Update SNMP Settings**.

Add an SNMP Notification Receiver

You can configure the RealPresence Resource Manager system to send SNMP messages to different notification receivers (e.g., a network management system).

Follow these guidelines when setting up notification receivers:

- When SNMP settings are set to SNMP v2c, you can set v3 INFORM receivers but not v3 TRAP receivers.
- When your SNMP settings are set to SNMP v3, v3 TRAP notifications automatically use the security (authentication and encryption) settings. However, you must set the security settings for v3 INFORM notifications independently of the SNMP system settings. In addition, each v3 INFORM receiver must have use a unique authentication user name.

To add an SNMP notification receiver to the system

1 Go to **Admin > Server Settings > SNMP Settings**.

2 In the **Notification RCVR Actions** section, click **Add**.

3 Configure these settings in the **New Notification Receiver** dialog box.

Setting	Description
IP Address	Specifies the IP address of the host receiver.
Transport	Specifies the transport protocol for SNMP communications to the host receiver. Possible values are: • TCP • UDP Select the transport protocol for which the host receiver is configured.
Port	Specifies the port that the RealPresence Resource Manager system will use to send notifications. By default, the RealPresence Resource Manager system uses port 162.

Setting	Description
Trap/Inform	Specifies the type of information that should be sent to the host receiver. Possible values are: • Inform—An unsolicited message sent to a notification receiver that expects/requires a confirmation message. Introduced with SNMP version 2c, this option is not supported by systems that only support SNMP version 1. • Trap—An unsolicited message sent to a notification receiver that does not expect/require a confirmation message.
SNMP Version	For SNMPv3, specifies the context for the information. The RealPresence Resource Manager system is a proxy-forwarding application. It passes SNMP requests to its various SNMP-reporting processes based on the context information in the SNMP message. For SNMPv3, this context is identified by `contextName` and `contextEngineID`.
Security User	For SNMPv3, specifies the security name required to access a monitored MIB object. **Note** The security user is only required for **Inform** notifications.
Auth Type	For SNMPv3, specifies the authentication protocol. The RealPresence Resource Manager system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB). Possible values for authentication protocol are: • MD5 • SHA These protocols are used to create unique fixed-sized message digests of a variable length message. MD5 creates a digest of 128 bits (16 bytes) and SHA creates a digest of 160 bits (20 bytes).
Auth Password	For SNMPv3, specifies the authentication password that is appended to the authentication key before it is computed into the MD5 or SHA message digest.

Setting	Description
Encryption Type	For SNMPv3, specifies the privacy protocol for the connection between the RealPresence Resource Manager system and the notification receiver. The RealPresence Resource Manager system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB). Possible values for privacy protocol are: • DES • AES **Note** • The **Encryption Type** is only required for **Inform** notifications.
Encryption Password	For SNMPv3, specifies the password to be associated with the privacy protocol. **Note** The **Encryption Password** is only required for **Inform** notifications.

Download RealPresence Resource Manager System MIB Package

The Polycom® RealPresence® Resource Manager system enterprise MIB relates information about the system. The information is divided into these categories:

- Configuration—The static state of each component, for example component type, software version, current owner, values of all configured parameters.
- Status—The dynamic state of each component, for example the number of connections, number of conferences, number of ports (used and available), temperature, fan speed, CPU utilization, memory utilization, network link status, number of dropped packets, jitter measurements, number of successful calls, number of CPU resets.
- Alerts—To notify that an exception condition has occurred, for example a power supply failure, link/down up on a major interface, memory usage exceeding a predefined percentage, connections in an MCU exceeding a threshold, a logical fault or ungraceful transition.
- Conformance—The historical trend for selected groups of data, for example conference load over time for an MCU, bandwidth consumed over time for a network device.

The RealPresence Resource Manager system provides the following MIBs for user in monitoring the system:

Polycom RealPresence Resource Manager-specific MIBs

Name	Description
POLYCOM_BASE-MIB	Includes initialization information for all RealPresence Resource Manage product-specific MIBs. You must load this MIB before POLYCOM-RESOURCE-SCHEDULER-MANAGEMENT
POLYCOM-RESOURCE-SCHEDULER-MANAGMENT	RealPresence Resource Manager-specific MIB definition.
POLYCOM-CMA-MIB	Contains Polycom CMA system legacy traps for backward compatibility. Some traps in this MIB are no longer supported. See the release notes for details on supported traps for this MIB.

Third-party MIBs adapted for Hardware Monitoring

Name	Description
adptInfo	The interface table (ifTable) shows addresses, physical addresses, names, descriptions etc. of the network interfaces
baspcfg	The interface table (ifTable) shows addresses, physical addresses, names, descriptions etc. of the network interfaces
baspStat	
baspTrap	
DcAsfSrv	Trap definitions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.

Name	Description
dcs3fru	Contains all the field replaceable unit names, serial numbers, and revisions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.
DcAsfSrv	Trap definitions for the Polycom-branded Dell server. For more information, see the Dell SNMP documentation.
dcs3rmt	Provides information about server administrator remote access.
dcstorag	Monitoring and information about the hard disks and RAID configuration on the server.
dellcm	
iDRAC-MIB	Information about iDrac, including data, alerts, and traps
INET-ADDRESS-MIB	A definition file for standard conventions included for reference.
INTELLAN	Information about the Intel LAN.
ITU-ALARM-TC-MIB	A definition file for standard conventions included for reference.
10892	The primary MIB for the Polycom-branded Dell server. It provides 36 traps from the server motherboard, including system type, voltages, and temperature readings. For more information, see the Dell SNMP documentation.
ITassist	IT assistant.
Dell-RAC-MIB	Information about the Dell Remote Access Controller.
RFC1213-MIB	RFC1213MIB definitions included for reference. The RealPresence Resource Manager system supports all but "egp".
SNMPv2-CONF	A definition file for standard conventions included for reference.
SNMPv2-SMI	A definition file for standard conventions included for reference.
SNMPv2-TC	A definition file for standard conventions included for reference.
iDRAC-MIB	.

To download the MIB package for a RealPresence Resource Manager system

1. Go to **Admin > Server Settings > SNMP Settings**.
2. Click **Download MIBs**.
3. In the **MIBs** dialog box, select the MIB of interest.
4. Click **Download MIB**.

Polycom recommends using a MIB browser to explore the RealPresence Resource Manager system MIB. The RealPresence Resource Manager system MIB is self-documenting including information about the purpose of specific traps and inform notifications.

Configuring Alert Settings

This chapter describes how to configure the Polycom® RealPresence® Resource Manager system to send alerts to users via E-mail for specific types of system and endpoint events. It includes these topics:

- Set Up Remote Alerts on page 476
- Configure Remote Alert Profiles on page 481
- Disable Remote Alerts on page 484

Set Up Remote Alerts

The RealPresence Resource Manager system remote alerts functionality is very flexible. It allows you to:

- Assign different severity levels to different classifications of RealPresence Resource Manager system and Endpoint alerts.
- Create different alert profiles so that different types of alerts can be sent to different people. So if you have administrators who specialize by device type (for example bridges, endpoints, or servers), you can create profiles that notify each type of administrator of failures related to those specific types of devices.

To set up remote alerts, you must complete the following tasks:

1. Set Up RealPresence Resource Manager System-generated E-mail Account on page 477.
2. Enable RealPresence Resource Manager System Remote Alerts on page 477.
3. Set RealPresence Resource Manager System Remote Alert Level Settings on page 477.
4. Set RealPresence Resource Manager System Alert Threshold Settings on page 479
5. Set Endpoint Alert Level Settings on page 479.
6. Add a Remote Alert Profile on page 481.
7. Associate a Remote Alert Profile With a User on page 483.

Set Up RealPresence Resource Manager System-generated E-mail Account

To set the RealPresence Resource Manager system-generated E-mail account

1. Go to **Admin > Server Settings > E-mail**.
2. On the **E-mail** page, enter the E-mail account (ASCII only) from which the Resource Manager system will send conference notification E-mails and system alerts.
3. Specify the IP address of the mail server from which the RealPresence Resource Manager system will send conference notification E-mails.

> - Many E-mail servers will block or discard E-mails without a qualified From: address. To avoid this issue, make sure each person with Scheduler permissions has a valid E-mail address.
> - Many E-mail servers will block or discard E-mails from untrusted domains, in which case you may need to change the default RealPresence Resource Manager system E-mail address to one in a trusted domain.

4. Click **Update**.

Enable RealPresence Resource Manager System Remote Alerts

To enable RealPresence Resource Manager system remote alerts

1. Go to **Admin > Alert Settings > Remote Alert Setup**.
2. On the **Remote Alert Setup** page, select **Enable Remote Alerts**.
3. Set a **Remote Alert quiescent time**, which is the amount of time (in minutes) the system should wait after alerts have been detected but not cleared before starting the alert notification process, and if applicable, the remote alert notification process.
4. Click **Update**.

Set RealPresence Resource Manager System Remote Alert Level Settings

The RealPresence Resource Manager system monitors and reports events regarding its performance, connections, and services. It categorizes alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the Alert Severity Level is set to **Info** for all of the **Resource Manager Alert Types** it reports. You have these options:

- You can leave all of the **Alert Severity Levels** set to **Info** and create a single remote alert profile that allows you to notify all users assigned that profile about system events of all types.
- You can change some of the **Alert Severity Levels** to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of system events of different types and severity levels.

To set the RealPresence Resource Manager system remote alert level settings

1 Go to **Admin > Alert Settings > Resource Manager Alert Level Settings**.

2 On the **Resource Alert Level Settings** page, change the **Alert Severity Level** for the following **Resource Manager Alert Type** system events, as required.

Alert Type	Alert indicates...
Bridge Down	A Polycom MCU has failed.
Database Connection Down	The connection to the database has been lost.
Enterprise Directory Connection Down	The connection to the enterprise directory server has been lost.
Enterprise Directory System Account Password Failure	The connection to the enterprise directory server could not be established because the account password was incorrect.
Resource Manager Failover Occurred	(In redundant RealPresence Resource Manager system configurations only.) The system has failed over from one system server to the other.
License Capacity Threshold Exceeded	The number of available seats defined by the installed license is within 5% of the total license capacity.
License Expired Warning	The license will expire in less than 30 days.
Bridge Time Discrepancy	A difference between the clock on the Polycom MCU and the RealPresence Resource Manager system clock.
Redundant Server Down	(In redundant RealPresence Resource Manager system configurations only.) The connection or synchronization between the primary and secondary server has been lost.
Redundancy Service Stopped	(In redundant RealPresence Resource Manager system configurations only.) The redundancy service has stopped.
Resource Manager Failover Occurred	The primary server failover occurred.
Site Bandwidth Threshold Exceeded	The site bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Subnet Bandwidth Threshold Exceeded	The subnet bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Site Link Bandwidth Threshold Exceeded	The site link bandwidth threshold, which is set at 90% of capacity, has been exceeded.
Certificate Expiration Warning	The specified certificate will expire in 30 days. If the certificate is not renewed within 30 days, the alert continues daily.
Certificate Expired Warning	The specified certificate has expired. The alert continues daily until the certificate is renewed or removed.
Database Backup Failure	The database backup has failed.

3 Click **Update**.

Set RealPresence Resource Manager System Alert Threshold Settings

You can configue alerts to be sent when the RealPresence Resource Manager system reaches certain thresholds. Each threshold is set to a default value that you can change.

To set the RealPresence Resource Manager Alert Thresholds

1 Navigate to **Admin > Alert Settings > Resource Manager Alert Threshold Settings**.

2 On the **Resource Manager Alert Threshold Settings** page, change the alert threshold for following threshold alerts.

Alert Threshold	Definition and Default Value
Used disk space threshold	Percentage of disk space that is used. Default threshold is 90 percent.
Memory usage alert threshold	Percentage of memory that is used. Default threshold is 95 percent
Average CPU usage alert threshold	Average percentage of CPU usage. Default threshold is 95 percent
Average CPU usage alert threshold window	Enter the threshold window of which to measure CPU usage. Default window is 10 minutes.
Average intrusion frequency alert threshold	Enter the threshold in number of intrusions per second. Intrusions can be measured up to two decimal points. For example 2.59. Default threshold is 1 intrusion per second.
Intrusion alert threshold window	Enter the threshold window of which to measure intrusion frequencies. Default threshold window is 1 minute.

Set Endpoint Alert Level Settings

Monitored endpoints send events to the RealPresence Resource Manager system. The RealPresence Resource Manager system categorizes and reports endpoint alerts into three alert levels: **Info**, **Minor**, or **Major**.

By default the **Alert Severity Level** is set to **Info** for all of the **Endpoint Alert Types** it reports. You have these options:

- You can leave all of the **Alert Severity Level**s set to **Info** and create a remote alert profile for each endpoint type being monitored that allows you to notify all users assigned that profile about all endpoint events applicable to that endpoint type.

- You can change some of the **Alert Severity Level**s to either **Minor** or **Major** and create multiple remote alert profiles that notify different users of endpoint events of different types and severity levels.

To set the endpoint alert level settings

1 Go to **Admin > Alert Settings > Endpoint Alert Level Settings**.

2 On the **Endpoint Alert Level Settings** page, change the **Alert Severity Level** for the different types of endpoint events as required.

Alert Type	Alert indicates...
Remote Control Battery Low	The battery in the endpoint's remote needs to be replaced.
Credentials Required	The endpoint system requires that the user enter a valid username and password.
Credentials Failed	An attempt to log into the endpoint system failed.
HTTP Forbidden	The endpoint must be used in `https:` mode only.
Device Not Responding	The endpoint is not responding to the RealPresence Resource Manager system.
Heartbeat Timeout	The endpoint did not send a heartbeat to the RealPresence Resource Manager system within the required timeout period.
Gatekeeper Status Unknown	The system gatekeeper cannot determine the connection status of the endpoint.
Gatekeeper Rejected	The gatekeeper rejected the endpoint's attempt to register.
Gatekeeper Unregistered	The endpoint is not registered to the gatekeeper.
Directory Status Unknown	The system gatekeeper cannot determine the directory status of the endpoint.
Directory Not Registered	The endpoint is not registered to the directory service.
Presence Status Unknown	The system gatekeeper cannot determine the presence status of the endpoint.
Presence Unregistered	The endpoint is not registered to the presence service.
User Assistance Request	The endpoint user sent a request for help.
Management URL Not Set	The RealPresence Resource Manager system is not one of the management URLs set on the endpoint, possibly because the management URL list is full. **Note** Because endpoint systems do not have an interface to manually delete management URLs, if the management list is full you must disconnect the endpoint's network cable for two minutes. This should clear up all the mgmt server URLs.
Touch Control Disconnected	The Touch Control device that was connected to the listed HDX is no longer connected to the HDX.

Alert Type	Alert indicates...
Touch Control Software Incompatible with Endpoint	The software version of the Touch Control platform is not compatible with the Endpoint software version.
SIP URI Not Provisioned	A dynamically-managed endpoint at a site with SIP enabled does not have a SIP dial string reservation. The endpoint is provisioned without SIP enabled.
SIP Status Unknown	The SIP server cannot determine the status of the endpoint.
SIP Unregistered	The endpoint is not registered with the SIP server.

3 Click **Update**.

Configure Remote Alert Profiles

Remote alert profiles identify which device alerts are included in alert settings. Note that using a combination of setting alerts by device type and by specific types, provides additional granularity in managing device alerts.

This section includes the following topics:

- Add a Remote Alert Profile on page 481
- Associate a Remote Alert Profile With a User on page 483
- Edit a Remote Alert Profile on page 483
- Disable a Remote Alert Profile on page 483
- Delete a Remote Alert Profile on page 484

Add a Remote Alert Profile

You can add a remote alert profile to identify which device alerts from which devices should be included in alert information.

To add a remote alert profile

1 Go to **Admin > Alert Settings > Remote Alert Profiles**.

2 On the **Remote Alert Profiles** page, click **Add**.

3 In the **Add Remote Alert Profile** dialog box, enter a **Name** and **Description** for the profile.

4 To activate the profile, mark the **Enabled** check box.

5 Configure one of the following:

➢ To have all RealPresence Resource Manager system alerts sent as part of this profile, select **Info**, **Minor**, *and* **Major**.

- ➢ To have a subset of RealPresence Resource Manager system alerts sent as part of this profile, select any combination of **Info**, **Minor**, or **Major**. These selections work in conjunction with the RealPresence Resource Manager system alert level settings you chose previously.
- ➢ To have no RealPresence Resource Manager system alerts sent as part of this profile, leave **Info**, **Minor**, *and* **Major** cleared**.**

6 To use the device type to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device Type** and configure one of the following. For endpoint systems, these selections work in conjunction with the endpoint alert level settings you choose previously.

a To have all device alerts for all device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select **Info**, **Minor**, *and* **Major** for all of the device types.

b To have a subset of device alerts for all device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select any combination of **Info**, **Minor**, or **Major** for each device type.

c To have all device alerts for a subset of device types sent as part of this profile, in the **Device Type Alert Level Mapping** page, select **Info**, **Minor**, or **Major** for each device type to be included in the profile. Alerts for those device types that do not have an alert level selected will not be included.

7 To use the device name to identify which devices and device alerts should be sent as part of this profile, click **Alert by Device**.

> - If you set device alerts for specific devices, these settings override settings made on the **Alert by Device Type** page. The settings are not cumulative.
> - You cannot set the system up to send device alerts for specific desktop video endpoints. Polycom CMA Desktop, RealPresence Desktop and RealPresence Mobile endpoints are not displayed in the **Available Device** list.

a As needed, use the **Filter** to customize the device list.

b In the **Available Devices** list, select the devices to add to the profile. Use CTRL to select multiple devices.

c Click the down arrow to add the devices to the **Monitored Devices** list and configure one of the following:

- ♦ To have all device alerts for all selected devices sent as part of this profile, for the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device**.**
- ♦ To have a subset of device alerts for all selected devices sent as part of this profile, for the devices in the **Monitored Devices** list, select any combination of **Info**, **Minor**, or **Major** for each device.
- ♦ To have all device alerts for a subset of device types sent as part of this profile, for the devices in the **Monitored Devices** list, select **Info**, **Minor**, and **Major** for each device to be included in the profile. Alerts for those devices in the **Monitored Devices** list that do not have an alert level selected will not be included.

8 Click **OK**.

Associate a Remote Alert Profile With a User

To associate a remote alert profile with a user

1 Go to **User > Users**.

2 To search for a user:

   a In the **Search** field of the **Users** page, search for the user of interest.

> Searches for a user on the RealPresence Resource Manager system **Users** page are case-insensitive, prefix searches of the **Username**, **First Name**, and **Last Name** fields.

   b To search both local and enterprise users, clear the **Local Users Only** check box and press **Enter**.

   The first 500 users in the database that match your search criteria are displayed in the **Users** list.

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

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

4 In the **Edit User** dialog box, click **Associated Alert Profile**.

5 Select the **Remote Alert Notification Profile** to associate with the user.

6 Click **OK**.

Edit a Remote Alert Profile

To edit a Remote Alert Profile

1 Go to **Admin > Alert Settings > Remote Alert Profiles**.

2 On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.

3 As required, edit the **General Info**, **Alert by Device Type,** and **Alert by Device** sections of the **Edit Remote Alert Profile** dialog box.

4 Click OK.

Disable a Remote Alert Profile

To disable a Remote Alert Profile

1 Go to **Admin > Alert Settings > Remote Alert Profiles**.

2 On the **Remote Alert Profiles** page, select the profile of interest and click **Edit Remote Alert Profile**.

3 Clear **Enable Profile**.

4 Click **Update**.

Delete a Remote Alert Profile

To delete a Remote Alert Profile

1 Go to **Admin > Alert Settings > Remote Alert Profiles**.

2 On the **Remote Alert Profiles** page, select the profile of interest and click **Delete Remote Alert Profile**.

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

The profile is deleted from the RealPresence Resource Manager system.

Disable Remote Alerts

You can disable all remote alerts.

To disable all (system and device) RealPresence Resource Manager system remote alerts

1 Go to **Admin > System Settings > Remote Alert Setup**.

2 On the **Remote Alert Setup** page, clear **Enable Remote Alerts**.

3 Click **Update**.

System Backup and Recovery

This chapter provides an overview of the Polycom® RealPresence® Resource Manager system backup and recovery procedures. It includes these topics:

- Create System Backups on page 485
- Restore the System on page 487

Create System Backups

Polycom recommends configuring automatic system backups to be archived weekly. This archive makes system restoration much simpler. You can configure automatic system backups in addition to being able to download a system backup at any time.

The backup and recovery of a RealPresence Resource Manager system includes backup and recovery of the RealPresence Resource Manager system internal database and the backup of the RealPresence Resource Manager system configuration settings.

Users assigned the **Administrator** role can create backups of the existing system. System backups are created in a `.zip` format which includes both the database backup files and the system settings.

This section includes the following topics:

- Creating an Automatic System Backup on page 485
- Creating a System Backup Manually on page 486

Creating an Automatic System Backup

Polycom recommends scheduling regular system backups. When you configure automatic system backups, the system backup zip file is automatically created and sent via FTP site to an external server. Be sure the external storage server has enough space to store regular backups. Verify the size of the backup file occasionally to ensure transfer success.

To schedule automatic system backups

1 Go to **Admin > Maintenance > Backup/Restore System Settings**.

2 Configure these settings:

Field	Description
Enable FTP of Auto System Backup	Mark this check box to enable automatic system backups to be sent to an external server via FTP.
Last Successful Transfer Time	Displays the date and time of the last time a system backup was successfully created and transferred.
Next Transfer Date	Use the calendar to set up the next transfer date.
Transfer Start Time	Set the start time of the next transfer and all subsequent transfers. Time format is in 24 hour format. For example, 22:00 is 11 p.m. Do not schedule system backups during peak server hours as it can affect system performance.
Auto System Backup Transmission Frequency (In Days)	Set the number of days between each transfer.
Host name or IP Address of FTP server	Specifies the server to which the system backup will be transferred.
FTP Port	Specifies the port through which the system backup will be transferred. By default, this is system port 21.
FTP User Name FTP Password Confirm FTP Password	Specifies a user name and password combination for accessing the FTP server. This must be a valid user account on the FTP server.
FTP Directory	Specifies the directory on the server to which the system backup will be transferred. The default directory is the root folder of the FTP server. If you want to use a different directory, you need to create that directory on the FTP server first. For example, create an `./AutoBackup` folder on the FTP server and then indicate that directory name as the FTP Directory in the RealPresence Resource Manager system.

3 To verify that the FTP settings are functional, click **Test Archive Settings**.

4 When the settings are correct, click **Save Settings**.

If the RealPresence Resource Manager system cannot contact the FTP server, the system generates an alert.

See Configuring Alert Settings on page 476

Creating a System Backup Manually

You can manually create a backup archive of a RealPresence Resource Manager system including system configuration settings and database files at any time. You can choose this option even if you have already configured automatic system backups.

When you choose this option, you must download the archive and save it to a location of your choice.

Once the backup archive is downloaded, it can be used to restore the system to its last archived configuration after a disastrous system failure.

> System archives do not include system and audit logs. If you want to archive these logs, you must do so separately.
>
> See Managing Audit Log Files on page 496

To manually create a system backup

1. From the RealPresence Resource Manager system web interface, go to **Admin > Maintenance > Backup/Restore System Settings**.
2. When the **Backup/Restore System Settings** page appears, click **Create and Download a Backup Archive**.
3. In the **Select location for download** dialog box, enter a unique **File name**, browse to a location on your system and click **Save**.

   A **File Download** dialog box displays the progress of the download operation.
4. When the operation is completed, click **OK**.
5. Browse to the location specified in step 3 and verify the file download.

Restore the System

A user assigned the **Administrator** role can restore a RealPresence Resource Manager system using a backup archive. To restore a RealPresence Resource Manager system, follow the procedures in this topic.

To restore a system from a backup archive

1. See Restore to Factory Default Image on page 488.
2. **Perform First Time Setup**. For more information about First Time Setup, see the *Polycom RealPresence Resource Manager System Getting Started Guide* for this release.
3. Restore from a Backup Archive on page 488 using the last archived configuration. The archived configuration will overwrite the configuration that resulted from **First Time Setup**. The only RealPresence Resource Manager system configuration settings not included in the archive and thus not overwritten are the network settings and the security certificates required for an operational system.

In cases when the RealPresence Resource Manager system is functional, but the configuration or database is corrupted, the backup archive can also be used to return a RealPresence Resource Manager system back to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the RealPresence Resource Manager system to its former functional state.

Restore to Factory Default Image

In a disaster recovery situation, your Polycom Global Services (PGS) support representative may be required to restore your RealPresence Resource Manager system to its factory default image.

To perform this disaster recovery procedure, you will need the **Restore to Factory Default DVD** that shipped with the RealPresence Resource Manager system server. This DVD has the base image of the RealPresence Resource Manager system server software.

> **WARNING**
>
> - This is a last resort, so never do this without being instructed to do so by PGS support.
> - This process will wipe out your system database and all other system data.
> - The **Restore to Factory Default DVD** is specific to the RealPresence Resource Manager system server type and version.

Restore from a Backup Archive

A user with the **Administrator** role can restore the RealPresence Resource Manager system using a backup archive.

When you restore from a backup archive:

- Do not allow users to connect to the server during the restoration process.
- The system restarts when the restoration process is finished.

To restore a backup archive

1 Go to **Admin > Maintenance > Backup/Restore System Settings**.

2 In the **Select Archive File** section of the **Backup/Restore System Settings** page, click ... .

3 Select the archive file to upload and click **Open**.

4 Click **Restore from Backup Archive**.

Two warnings appear about the backup process. The second warns that the process is irrevocable and may result in an usable system.

5 Click **OK**.

The system uses the archive file to restore the RealPresence Resource Manager system to the state of the backup files.

When the RealPresence Resource Manager system is functional, but the configuration or database is corrupted, you can also use these steps to return a RealPresence Resource Manager system to its last known good archive. As long as the network settings and security certificates are operational, the last known good archive will return the RealPresence Resource Manager system to its former functional state.

System Maintenance and Troubleshooting

This chapter provides Polycom® RealPresence® Resource Manager system troubleshooting information. It includes the following topics:

- System Log Overview on page 489
- Managing Locally Stored System Logs on page 490
- Managing System Logs using a Syslog Server on page 493
- Managing Audit Log Files on page 496
- Troubleshooting Utilities Dashboard
- Resource Manager System Report on page 499
- Troubleshooting Specific Types of Issues
  - Registration Problems and Solutions
  - Point-to-Point Calling Problems and Solutions
  - MCU and Gateway Dialing Problems and Solutions

System Log Overview

The detailed technical data in the system log files can help Polycom Global Services resolve problems and provide technical support for your system.

In such a situation, your support representative may ask you to download log archives and send them to Polycom Global Services. You may be asked to manually roll logs in order to begin gathering data anew. After a certain amount of the activity of interest, you may be asked to download the active logs and send them to Polycom Global Services.

You can choose to store system logs on your local server in addition to using an external syslog server, according to parameters you choose.

For more information about system maintenance, see System Management and Maintenance on page 444.

System Log Overview

The RealPresence Resource Manager system manages the following system logs:

System Log	
Jserver	XMA application log. The log file that shows information related to the internal LDAP, SNMP, DM, XMPP, Site Topology and dynamically-managed endpoint login and provisioning functionality.
DeviceManager	Log file for the device management process.
Conference	Conference scheduling log used by the conference scheduling process. This log contains debug information on how a conference is created.
Corosync	Redundancy log that records redundancy status and activity such as corosync, pacemakers, dataeng, lrmd and so on.
Redundancy	Redundancy log that record related information once a failover has occurred.

Managing Locally Stored System Logs

When you choose to store system logs on the local RealPresence Resource Manager system, you can easily download them directly from the system, customize the logging settings, as well as determine how often the logs are restarted (rolled).

- View Locally Stored System Log Files on page 490
- Change Logging Level for Locally Stored Logs on page 491
- Download Locally Stored Log Files on page 492
- Roll Locally Stored Log Files on page 492

View Locally Stored System Log Files

Many of the RealPresence Resource Manager system components can write a **System Log File** when they experience an error or issue.

To view system log files

1. Go to **Admin > Maintenance > 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**.

      The log file is downloaded and can be opened for viewing.

Change Logging Level for Locally Stored Logs

You can configure the log level for the following system logs:

- Jserver
- DeviceManager
- Conference

To edit the current system log level for local logs

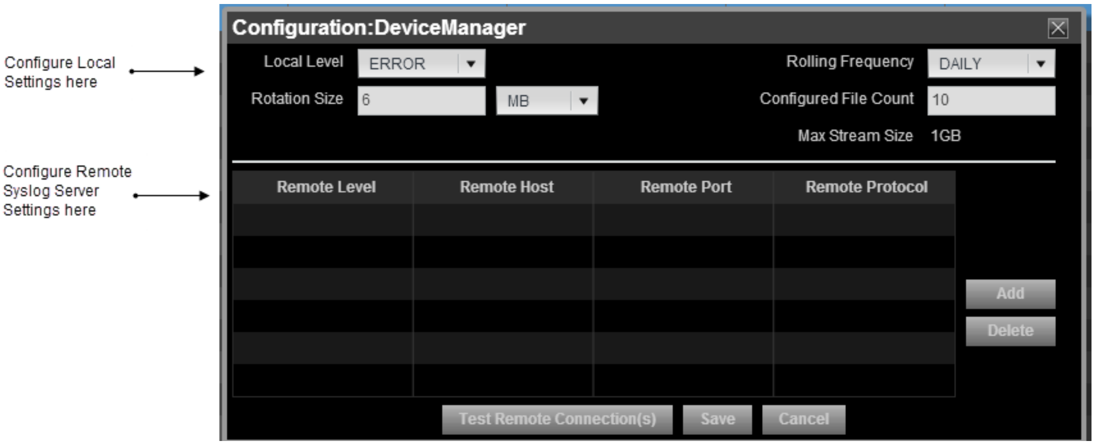
1 Go to **Admin > Maintenance > Log Settings**.

2 The **System Log Files** list appears.

3 Select log you want to change.

4 Click **Edit**.

5 In the **Configuration:** dialog, you can modify the settings of locally stored system log files as well as specify if the log file gets sent to a remote syslog server. For instructions on setting remote syslog settings, see Storing a System Log on a Remote Syslog Server on page 493.



Configure Local Settings here

Configure Remote Syslog Server Settings here

Configuration:DeviceManager

Local Level: ERROR

Rotation Size: 6 MB

Rolling Frequency: DAILY

Configured File Count: 10

Max Stream Size: 1GB

Remote Level	Remote Host	Remote Port	Remote Protocol

6 Configure the following settings for the specified file. If you set the local level to **None**, no log file will be stored.

Field Name	Description
Local Level	Sets the logging level for the system log file stored on the local server. Logging levels include: • None • Emergency • Alert • Critical • Error • Warning • Notice • Information • Debug
Rotation Size	Configures the maximum size the log file can reach before it is rolled.
Configured File Count	Configures the maximum number of this type of log file that can be stored on the local server.
Rolling Frequency	Configures how often the log file is rolled. When a log file is rolled, a new log file is started and the previous log file is archived on the local server.

7 Click **Save**.

Download Locally Stored Log Files

You can download a .gz file that includes the log files for the RealPresence Resource Manager system. The log files include the operating system level application, security, and system logs. These logs store events logged by the operating system.

To download the System Logs

1 Go to **Admin > Maintenance > System Log Files**.

2 Click **Download All**.

3 To open the `.gz` file, in the **File Download** dialog box, click **Open with**, and browse to the program you use to open.`zip` files.

4 To save the `.gz` file to your local computer, in the **File Download** dialog box, click **Save**.

Roll Locally Stored Log Files

You can use the **Roll Log** action to close and archive locally stored log files and start new log files.

Although you can configure an automatic window in which logs are rolled (restarted), you can also manually roll the logs whenever you need to troubleshoot a particular incident.

When you roll locally-stored logs, the following subset of locally-stored logs are archived and restarted.

- Jserver
- DeviceManager
- Conference
- Corosync
- Redundancy

For more information about what these logs contain, see System Log Overview on page 489.

To roll the system logs

1. Go to **Admin > Maintenance > System Log Files**.
2. Click **Roll Logs**.

   A message displays confirming the operation and detailing which logs were rolled.
3. Click **Ok**.

Managing System Logs using a Syslog Server

If your IT environment includes an external syslog server, you can choose to have system logs automatically sent to that server to be stored and managed externally from the RealPresence Resource Manager system.

This section includes the following topics:

- Storing a System Log on a Remote Syslog Server on page 493
- Deleting a Log from Being Stored on a Remote Syslog Server on page 495

Storing a System Log on a Remote Syslog Server

You can select individual logs and choose to have them stored on a remote syslog server. Logs can be stored both locally and on a syslog server at the same time. You can use both methods if you want to customize log settings.

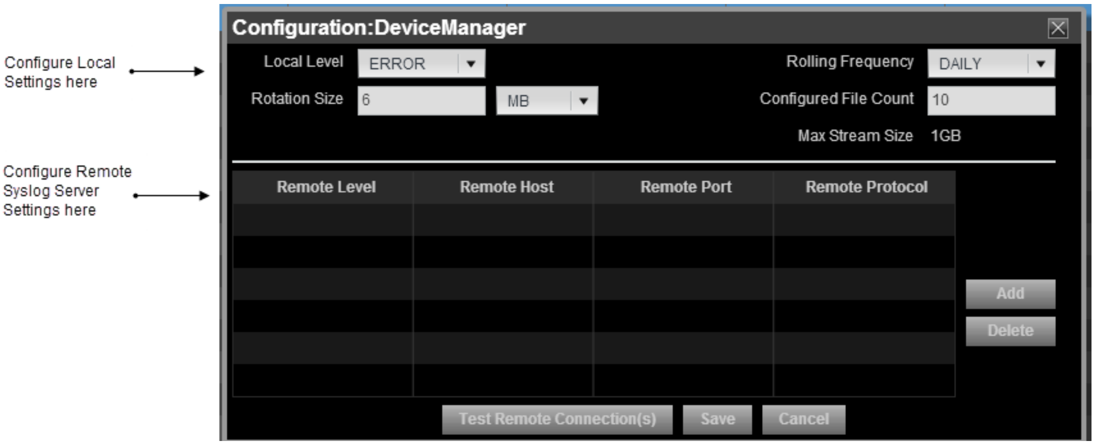
Note

The corosync.log and redundancy.log include database information that cannot be completely stored on a remote syslog server. Please defer to locally stored files for complete information about redundancy issues.

To configure a system log to be sent to a remote syslog server

1. Go to **Admin > Maintenance > Log Settings**.
2. The **System Log Files** list appears.
3. Select log you want to change.
4. Click **Edit**.

5 In the **Configuration:** dialog, you can specify if the log file gets sent to a remote syslog server or modify the settings of locally stored system log. For instructions on setting remote syslog settings, see Change Logging Level for Locally Stored Logs on page 491.



Configure Local Settings here

Configure Remote Syslog Server Settings here

Configuration:DeviceManager

Local Level: ERROR

Rotation Size: 6 MB

Rolling Frequency: DAILY

Configured File Count: 10

Max Stream Size: 1GB

Remote Level	Remote Host	Remote Port	Remote Protocol

6 Click **Add**.

7 In the **Remote Level** column, select a log level.

8 In the **Remote Host** column, enter the IP address of the syslog server you want to use.

9 In the **Remote Port** column, enter the port you want to use on the syslog server.

10 In the **Remote Protocol** column, enter the transport protocol you want to use (TLS, UDP, TCP).

11 Click **Test Connection** to verify that the log server is configured correctly.

12 Click **Save**.

Deleting a Log from Being Stored on a Remote Syslog Server

When you delete the remote settings for a system log, it is no longer sent to the syslog server for storage.

To undo remote storage of a system log

1. Go to **Admin > Maintenance > Log Settings**.
2. The **System Log Files** list appears.
3. Select log you want to modify.
4. Click **Edit**.
5. In the **Configuration:** dialog, select the remote server settings that you want to delete and click Delete.
6. Click **Save**.

Managing Audit Log Files

Audit logs provide a way to monitor the system for security and system access activity.

The following table identifies the RealPresence Resource Manager system audit log files.

Log Name	Description
localhost_access.log	Log file that shows every web request that was made from client systems. The system may have more than one such log.
ResourceManager_audit_jserver.log	Log file that captures security-related authentication issues.
kernel.log	Logs are useful not only for understanding the internal operation of a system but also the timing and relationships of activities within the system through the time-ordered messages within a time-stamped log.
hids.log	Log file that captures intrusion detection alerts.

For more information about the auditor role, see Auditor Responsibilities on page 445.

This section includes the following topics:

- View and Download Audit Logs on page 496
- Change Audit Log Settings on page 497
- Roll Audit Logs on page 497
- Backup and Delete Audit Files on page 497

View and Download Audit Logs

You can view and download audit log files.

To view and download audit log files

1. Go to **Admin > Maintenance > Audit Log Files**.

   The **Audit Log Files** page appears listing the logs being stored on the system.
2. Select the audit log of interest and click **Open**.
3. In the **File Download** dialog box, click **Open** to view the file or click **Save** to save the log file to your local system.

Change Audit Log Settings

Audit logs are automatically kept and stored until the maximum storage amount is of 2 GB is reached. You can configure alerts to be sent when the audit logs reach a specified percentage of the maximum storage available.

Audit logs are automatically rolled, archived, and the oldest logs deleted when the 90 percent of the storage (1.8 GB) is used. An alert is sent to the alert email address you have configured (see Edit the System E-mail Account on page 345).

To set an alert for audit log storage

1. Navigate to **Admin > Audit Log Files**.
2. In the ACTIONs section, click **Change Settings**.
3. In the **Audit Log File Setting** dialog box, configure the percentage of file size usage you want to reach before being alerted. You can set a percentage between 40 and 80 percent of the maximum storage amount of 2 GB.
4. Click **Ok**.

Roll Audit Logs

You can archive logs and restart them at any time. This process is called rolling. When you roll audit logs, each existing log is zipped and stored as a .gz file that can be backed up and deleted from the system. To back up and delete archived logs, see Backup and Delete Audit Files on page 497.

Audit logs are automatically rolled, archived, and the oldest logs deleted when the 90 percent of the storage (1.8 GB) is used. An alert is sent to the alert email address you have configured (see Edit the System E-mail Account on page 345).

Current logs maintain an extension of `.log` while archived logs are stored as `.gz` files.

To roll audit logs

1. Navigate to **Admin > Audit Logs**.
2. In the ACTIONs section, click **Roll Logs**.

   A message dialog informs you that the audit log files were successfully rolled.
3. Click **Ok**.

Backup and Delete Audit Files

The RealPresence Resource Manager system allows you to store audit logs locally until the maximum file storage limit of 2 GB is met. You should periodically roll the logs, and then backup the archived files and delete them from the local system.

You can create a backup of audit files and then delete the files from the server. After you create a backup (a zip fiile) you are prompted to verify that the files are authentically from the server from which they were downloaded and have not been modified since being downloaded. You need to verify the zip file with the Polycom Verification Utility which is provided.

You must have the auditor role in order to download and delete audit log files.

To backup and delete audit files

1. Navigate to **Admin > Maintenance > Audit Log Files**.
2. Click **Backup and Delete** in the ACTIONS pane.
3. In the **Backup and Delete** dialog box, ensure that each audit log file that you want to backup is marked. All audit logs are marked by default, you can unmark the files that you do not want to include in the archive.
4. Click **Backup**. The files you selected and downloaded to a zip file.

   Save the downloaded zip file to a location on your hard drive or network.
5. Click **Download Verification Utility**.

   The Polcyom File Verification Utility generates a checksum number that can be used as a verification code to ensure that the audit log files have not been modified after they were downloaded.
6. Execute the File Verification Utility and browse to the location of the audit file backup. After doing so, the File Verification Utility will output a value that can be copied to the clipboard.
7. Copy the **Verification Value** and enter it into the **Verification Code** section of the RealPresence Resource Manager system dialog box.
8. Click **Verify and Delete**.

   The audit logs are deleted from the RealPresence Resource Manager system.

Resource Manager System Report

The **Resource Manager System Report** can be a useful report. It produces a `SystemInfo.txt` file that describes the system configuration.

To view the Resource Manager System Report

1. Go to **Admin > Maintenance > Troubleshooting Utilities**.
2. In the **Resource Manager System Report** section of the **Troubleshooting Utilities** page, click **Download Report** in the **Resource Manager System Report** section.
3. When the **File Download** dialog box appears, either **Open** or **Save** the `SystemInfo.txt` file:

   The report includes this information.

```
RESOURCE MANAGER VERSION
     Software version  :  8.1.0.0_12-135102
     Hardware version  :  UNKNOWN
     LDAP Integration  :  false

SECURITY SETTINGS
     System under Secure Mode:  false

NETWORK CONFIGURATION
     System name           :  XMA-114
     System DSCP tag       :  0
     System IPv4 Address   :  10.220.202.114
     System IPv6 Address   :  N/A
     System IPv6 Link local:  N/A
     System subnet mask    :  255.255.255.0
     System default gateway:  10.220.202.254
     System DNS domain     :  pct-cmaqa.com
     System DNS server 1:  172.21.120.179
     System DNS server 2:  N/A

LICENSE INFO
     Total number of licenses  :  100
     Number of licenses in used:  0

CONFERENCE SETTINGS
     Conference Time Warning                   :  true
     Include Conference Owner in new Conference:  false
     Allow Overbooking of dial-In participants :  false
     Conference PIN Length                     :  6

SESSION MANAGEMENT SETTINGS
     Remote Access Connection is allowed     :  true
     Resource Manager User Interface timeout (in sec):  0
     Max number of sessions per user          :  5
     Max number of sessions per user enabled  :  false
     Max number of sessions per system        :  50

LOCAL USER ACCOUNT CONFIGURATION
     Failed login threshold             :  3
     Failed login windows (hours)       :  1
     Lockout duration (minutes)         :  Indefinite
     Account Inactivity threshold (days):  -1

LOCAL PASSWORD REQUIREMENTS
     Maximum password age (days)     :  180
     Password warning interval (days):  7
     Number of lowercase letters     :  1
     Number of uppercase letters     :  1
     Minimum length (characters)     :  8
     Minimum password age (days)     :  1
     Number of numbers               :  1
     Reject previous passwords       :  8
     Number of special characters    :  1
     Minimum number of  changed characters  :  1
     Maximum consecutive repeated characters:  1

CERTIFICATE INFO
     Certificate Settings                :  N/A
     Cipher Suite                        :  STANDARD_MODE
     Allow Server Self Signed Cert       :  true
     Require Clents Send Certificate     :  false
     External Server Settings            :  N/A
     Trust Server Self Signed Certificate :  false
     Validate Server's hostname          :  false
     Validate Server's Date Range        :  false
     Validate Server's Revocation        :  false
     External Client Settings            :  N/A
     Trust Client Self Signed Certificate:  false
     Validate Client's Date Range        :  false
     Validate Client's Revocation        :  false
     Certificate Common Name    :  Resource Manager Self-Signed Certificate
     Certificate Alias          :  1
     Certificate Issuer         :  Resource Manager Self-Signed Certificate
     Certificate Common Name    :  XMA-114.pct-cmaqa.com
     Certificate Alias          :  default
     Certificate Issuer         :  XMA-114.pct-cmaqa.com

REDUNDANCY INFORMATION
     Server 1 IP address:  N/A
```

```
        Server 1 is Active:  false
        Server 1 is ON     :  false
        Server 2 IP address:  N/A
        Server 2 is Backup:  true
        Server 2 is ON     :  false
        Virtual IP address :  N/A

   DATABASE CONFIGURATION
        Use external DB     :  false
```

Troubleshooting Utilities Dashboard

The RealPresence Resource Manager system has a **Troubleshooting Utilities** dashboard that brings together on one page access to all of the information you might need to diagnose system issues. It includes access to various diagnostic files and informational panes.

The diagnostic files include:

- **Traces**—Use this option to generate and download a network sniffer trace that can help you examine the traffic to and from the RealPresence Resource Manager system.
- **Resource Manager System Logs**—Use this option to generate and download a `GetAllLogs.zip` file that includes all of the RealPresence Resource Manager system log files. For more information about these system logs, see Managing Audit Log Files on page 496.
- **Resource Manager System Report**—Use this option to generate and download a `SystemInfo.txt` file that describes the system configuration. For more information about this report, see Resource Manager System Report on page 499.
- **Test Network Connection**—Use this option to perform a **Traceroute** or **Ping** operation. **Traceroute** allows you to investigate the route path and transit times of packets as they travel across an IP network. **Ping** allows you to test the availability of a host on an IP network.
- **Synchronize Certificate Stores**—Use this option to reset all certificate stores with the currently uploaded certificates.

The information panes include:

- **Systems**—Displays summary information about the devices registered with the RealPresence Resource Manager system. For more information, see Systems on page 365.
- **Resource Manager Configuration**—Displays information about the configuration of the RealPresence Resource Manager system. For more information, see Resource Manager Configuration on page 362.
- **Resource Manager Info**—Displays general information about the RealPresence Resource Manager system. For more information, see Resource Manager Info on page 362.
- **Resource Manager Licenses**—Displays information about how the RealPresence Resource Manager system is licensed. For more information, see Resource Manager Licenses on page 363.
- **DMA**—Displays information about the Polycom DMA system as a gatekeeper.
- **Users Logged In**—Displays the type and number of users that are currently logged into the system. For more information, see Users Logged In on page 361.

Troubleshooting Specific Types of Issues

This section describe describes information on troubleshooting specific types of issues on the RealPresence Resource Manager system. It includes these topics:

- Registration Problems and Solutions on page 504
- Point-to-Point Calling Problems and Solutions on page 505

- MCU and Gateway Dialing Problems and Solutions on page 505

Registration Problems and Solutions

Problem	Description	Solutions
Unable to place calls to an MCU conference room from a registered Polycom HDX system	The dynamic management mode RealPresence Resource Manager system rejects the ARQ stating that the “endpoint is not registered” to the gatekeeper even though the system indicates it is registered.	• The MCU is not registered to the gatekeeper
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 Network Topology > 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 RealPresence Resource Manager system is restarted, some registrants that were previously online are now offline.	Some endpoints do not re-register when the RealPresence Resource Manager system goes down. Some MCUs do not reregister automatically after two retries.	• Reboot the MCU.

Point-to-Point Calling Problems and Solutions

Problem	Description	Solutions
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 Network Topology > 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.

MCU and Gateway Dialing Problems and Solutions

Problem	Description	Solutions
Call fails when using an MCU service. Dialing an MCU service results in a network error.	The call using the MCU service is rejected because of one of the following: • The MCU is not registered. • The MCU is offline. • The MCU prefix is not registered as an E.164 alias. • The MCU resource issue was sent through resource allocation indication or resource allocation.	• Verify that the MCU is registered. • Verify that the MCU is online. If the device is offline, reboot it.

Diagnostics for your Dell Server

If your RealPresence Resource Manager system is shipped with a Dell D620 server, you need to have a USB keyboard and a monitor in order to run diagnostics.

Perform these diagnostics only under the guidance of Polycom Global Services.

System Security and Port Usage

This section provides an overview of the port usage and security required by the Polycom® RealPresence® Resource Manager system and includes a comprehensive list of services and clients on the system that are required for normal operation. It includes these topics:

- Open Inbound Ports on the RealPresence Resource Manager System
- Outbound Ports Used by the RealPresence Resource Manager System

Open Inbound Ports on the RealPresence Resource Manager System

The following table lists the open inbound ports on the RealPresence Resource Manager system and provides a description of their use.

Port	Description
TCP 80	HTTP web server, through which the web application displays and where Polycom endpoints post status messages
TCP/UDP 161	SNMP listener
TCP 389	Directory services (LDAP)
TCP 443	HTTPS web server listener
TCP 700	(Polycom proprietary service) Service monitor for redundant RealPresence Resource Manager system servers
TCP 3601	(Polycom proprietary service) Global Address Book listener with which endpoints register
TCP 3389	Remote access
TCP 5222	Presence service (XMPP)
TCP 4449	(Polycom proprietary service) OpenDS (Data store for site topology) admin port
TCP 8989	(Polycom proprietary service) OpenDS (Data store for site topology) replication port

Third-party port-scanning software may incorrectly identify the Polycom proprietary services as IANA-registered services, since identification is made by port number only and not by the actual protocol being transmitted.

Outbound Ports Used by the RealPresence Resource Manager System

The following table lists all outbound ports that the RealPresence Resource Manager system uses to communicate with other systems, including endpoints, bridges, database servers, and other network equipment.

Port	Description
TCP 20	Used to FTP data to endpoints
TCP 21	
TCP/UDP 24	Used to access the telnet interfaces on endpoints
TCP/UDP 25	Used to send E-mail messages to SMTP servers
TCP/UDP 53	Used to access domain name servers (DNS)
TCP 80	Used to access the web application on endpoints
TCP 135 TCP 137 TCP 139	Active Directory (AD) Single Signon (NetBios/NTLM)
TCP/UDP 389	Used to access directory (LDAP) services
TCP 443	Secure access to endpoint devices (SSL) including Polycom CMA Desktop.
TCP 445	Active Directory Single Sign-on
TCP/UDP 636	Used to access LDAP over TLS/SSL (LDAPS)
TCP/UDP 3268	Used to access the Microsoft Active Directory Global Catalog using StartTLS
TCP/UDP 3269	Used to access the Microsoft Active Directory Global Catalog using LDAP-S