Polycom

Administrator's Guide

3.1 | January 2014 | 3725-78703-001C

Polycom® RealPresence® Access Director™ System

Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

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

Patent Information

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

End User License Agreement

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

The EULA for this product is available on the Polycom Support page for the product.

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

Contents

About This Guide

The *Polycom® RealPresence® Access Director™ System Administrator's Guide* is for system administrators who need to configure, monitor, maintain, and troubleshoot the Polycom RealPresence Access Director system.

System Administrator Required Skills

This content is written for a technical audience. As a system administrator of the RealPresence Access Director system, you must know the following:

- Basic computer and network system administration skills
- Network configuration, including IP addressing, subnets, gateways, domains, DNS, time servers, and possibly network routing rules
- Basic understanding of firewalls and network security
- The deployment model for the Polycom RealPresence Access Director system being installed and the video conferencing/collaboration network of which it will be a part

If necessary, obtain the assistance of the appropriate IT or network administration personnel before proceeding.

Related Documentation

Please read all available documentation before you install or operate the system. Documents are available at http://support.polycom.com.

- *Polycom RealPresence Access Director Release Notes*
- *Polycom RealPresence Access Director Getting Started Guide*
- *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*

Overview of the Polycom® RealPresence® Access Director™ System

This following topics provide an overview of the Polycom® RealPresence® Access Director™ system:

About the Polycom RealPresence Access Director System

The RealPresence Access Director system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP and H.323 calls from registered users, guests, and federated enterprises or divisions from both AVC and SVC endpoints. The system provides secure communication between remote users and offices, and among guest users and organizations outside of the client's enterprise network.

The RealPresence Access Director system integrates with the following Polycom components and endpoints.

- Polycom® RealPresence® Resource Manager systems provide management, provisioning, directory, and presence services.
- Polycom® RealPresence® Distributed Media Application™ (DMA™) systems serve as a central call control platform for SIP, H.323, and bridge virtualization, and act as H.323 gatekeepers.
- Polycom® RealPresence® Collaboration Server® systems serve as high-scale bridges for SIP and H.323 calls and support content over video.
- Polycom® RealPresence® CloudAXIS™ Suite
- Polycom® RSS™ systems enable recording of video, audio, and content.
- Polycom® RealPresence® Desktop supports sharing of video, audio, and content from your desk.
- Polycom® RealPresence® Mobile enables tablets and smartphones to connect to video and audio conferencing and to share content.
- Polycom® RealPresence® Content Sharing Suite
- Polycom® RealPresence® Group Series 300/500 Endpoints

- Polycom® HDX endpoints

Features and Capabilities

The RealPresence Access Director system offers the following key features:

SIP Back-to-Back User Agent

The RealPresence Access Director system serves as a SIP back-to-back user agent (B2BUA) and operates between both end points of a SIP video call session. When a SIP call takes place, the RealPresence Access Director system divides the communication channel into two call legs and mediates all SIP signaling between both ends of the call, from call establishment to termination.

The RealPresence Access Director system SIP B2BUA supports the following call scenarios:

- SIP remote users with both AVC and SVC endpoints
- SIP guest users with both AVC and SVC endpoints
- SIP enterprise-to-enterprise federated calling for AVC and SVC endpoints

H.323 Signaling Proxy

- H.323 remote users with H.460 endpoints
- H.323 guest users
- H.323 enterprise-to-enterprise neighbored calling

Media Relay

- RTP and SRTP pass through

Access Proxy

- Management, RealPresence CloudAXIS Suite, and other HTTPS application servers
- Presence (XMPP)
- Directory (LDAP)
- Passthrough reverse proxy to servers not supported by other access proxy protocols.
- HTTP tunnel (SIP signaling and media relay for SIP guest call HTTP requests from RealPresence CloudAXIS Suite clients)

Security

- Deployable behind outside firewalls that use Network Address Translation (NAT)
- Secured communications (TLS and certificates)
- Secure management (Syslog, LDAP authentication, and role-based access control)
- Server-side authentication

- Server-side session management
- Robust SIP TLS cipher
- OS hardening

Operating System

- CentOS 5.7 (2.6.18-274.el5)

Performance

- 1,000 simultaneous calls
- 600-700 MB throughput
- 5,000 concurrent registrations
- 20 call attempts per second for SIP calls
- 10 call attempts per second for H.323 calls

Endpoints (AVC and SVC)

- HDX systems
- RealPresence Group Series 300/500
- RealPresence Mobile
- RealPresence Desktop

Getting Started in the RealPresence Access Director System

These topics provide a general introduction for using the RealPresence Access Director System:

Logging Into and Out of the System User Interface

To log into the RealPresence Access Director system

1. Open a browser window and in the **Address** field, do one of the following:
   - If you specified your system IP address during initial installation and network configuration, enter your IP address.
   - If you did not specify your system IP address during initial installation and network configuration, enter the RealPresence Access Director system default IP address:

     `https://192.168.1.254:8443`
2. When the **Log In** screen appears, enter the following:
   - User ID: `admin`
   - Password: `Polycom123`

     The user ID `admin` and password `Polycom123` are the default log-in credentials after the initial installation of the system.

During any log-in attempt, if you enter the wrong credentials three times in a row, you must wait one hour before trying to log in again.

To log out of the RealPresence Access Director system

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

Working with Administrator Accounts

One administrator account is created during the initial installation and configuration of the RealPresence Access Director system.

Polycom recommends that the system administrator create at least one new administrator account with personal log-in information, and add other user accounts as needed. The administrator account created during installation should then be deleted.

To add a new administrator account

1. Go to **User > Users > Add**.
2. In **General Info**, complete the following fields:

Field	Description
First name	User's first name
Last name	User's last name
User ID	User's login name

Field	Description
Password	User's system login password
Confirm Password	Repeat user's system login password

3 Click **Associated Roles** and select **Administrator**.

4 Click the right arrow to add the role to the **Selected roles** list.

5 Click **OK**.

To delete the original administrator account

1 Go to **User > Users**.

2 Select the administrator account that was created during the initial installation of the system.

3 Under **Actions**, click **Delete**.

4 In the **Confirm Action** dialog box, click **Yes** to delete the account.

For additional information on managing local user accounts, see User Management on page 103.

Changing Your Password

To change your system password

1 Go to **User > Users**.

2 Select your account from the list of users.

3 Under **Actions**, click **Edit**.

4 Enter your new password in the **Password** and **Confirm Password** fields, according to the following requirements:

- The password length must be 9-20 characters.
- The password must contain at least one upper case letter, one lower case letter, and one number.

5 Click **OK**.

Using the Dashboard

When you log into the RealPresence Access Director system, the dashboard displays a menu bar and different panes that show system activity levels and settings.

You can customize the default dashboard to display the panes you want to view. The system saves your settings for subsequent logins.

The following default dashboard panes display after you log into the system:

- **Server Information**. This pane displays the amount or percentage of:
  - CPU Utilization
  - Total Memory

  - Used Memory
  - Total Disk
  - Used Disk
- **Services Status**. This pane shows whether the following services are running:
  - Access Proxy
  - SIP
  - H323
  - Media Relay
  - Two-box Tunnel
  - Database

The tunnel service status displays only if you deploy two RealPresence Access Director systems in a tunnel configuration.

- **License Status**. This pane displays call and bandwidth information:
  - Maximum Allowed Calls
  - Active SIP Calls
  - Active H.323 Calls
  - Active SIP Bandwidth
  - Active H.323 Bandwidth
- **Peak Call Monitoring.** This pane displays the percentage of peak calls for:
  - H323
  - SIP

Monitoring System Alerts

In addition to the default panes, the **System Alerts Pane** provides alerts when certificates are close to their expiration date or have expired. When alerts occur, the **System Alerts** button turns red and displays the current number of alerts.

The RealPresence Access Director system identifies two levels of alert.

- WARN: The system currently functions correctly, but resolving the issue identified in the alert is highly recommended before it becomes critical.
- CRITICAL: The system is not functioning correctly. Take immediate action to resolve the issue.

The table below defines the system issues that trigger an alert and the action to take to resolve an issue.

System Component	Alert Level	Reason for Alert	Action
Certificates	WARN	• The key store certificate will expire within 30 days.	• Go to **Admin > Certificates**. • Click **Refresh** next to the key store certificate. ➢ The certificate is renewed for one year.
		• The trusted certificate will expire within 30 days.	• Submit a new Certificate Signing Request (CSR) within 30 days. ➢ See Creating a Certificate Signing Request on page 45.
	CRITICAL	• The key store certificate expires while the RealPresence Access Director system is running.	• Restart and the system automatically generates a new self-signed certificate. **Note** If the key store certificate expires when the RealPresence Access Director system is not running, the system automatically generates a new self-signed certificate when the system is started again. No alert displays.
		• The trusted certificate has expired.	• Immediately submit a new CSR.

To open and close the System Alerts Pane

» Click the **System Alerts** tab on the bottom right of the dashboard.

To add panes to the dashboard

1 Click **Add Panes**.

2 From the menu, select the panes you want to display.

To close or resize a pane

1 Click  .

2 Click  to maximize.

3 Click  to restore the default size.

To set the refresh interval for the dashboard display

» On the 

button, click the down arrow to select a refresh interval.

The dashboard refreshes based on the interval you selected.

To return to the dashboard from other functions

» Click  .

Working with Menus

When you log into the RealPresence Access Director system as an administrator, all of the system menus display. Click the down arrow next to each menu to access the functions for that menu.

When configuring settings for the RealPresence Access Director system, all fields with a red asterisk (*) next to the field name are mandatory to complete.

The table below lists all of the menus and their corresponding functions (submenus).

Menu	Submenu
User	
	Users
Configuration	
	Access Proxy Settings
	SIP Settings
	H.323 Settings
	Media Traversal Settings
	Federation Settings
	Two-box Tunnel Settings
	Access Control List Rules
	Access Control List Variables
	Access Control List Settings
Maintenance	
	License
	Software Upgrade
	Shutdown and Restart
	Backup and Restore

Menu	Submenu
Admin	
	Network Settings
	Time Settings
	Certificates
	Security Settings
	Log Settings
	SNMP Settings
	History Retention Settings
	Port Range Settings
	Polycom Management System
	Microsoft Active Directory
Diagnostics	
	Active Call
	Call History
	Registration History
	System Log Files
	Traffic Capture
	Ping
	Traceroute
Help	
	About RPAD
	Help Contents

If you deployed two RealPresence Access Director systems in a tunnel configuration, one system acts as a tunnel server and the other as a tunnel client. The user interfaces for each of these systems differ and do not include all submenus.

Using Online Help

The RealPresence Access Director system provides context-sensitive help. You can access help content in the following ways:

- When you select a function from one of the menus, click the help icon at the top of page to access the help contents for that page.

- Within a window that requires you to enter information, click **Help** to display the specific help contents for that window.
- Open **Help Contents** to view a full listing of help topics.

To use Help Contents

1. From the dashboard, click **Help > Help Contents**.
2. In the **Contents** tab, click a topic to display the help information.
3. In the **Search** tab, enter a word or phrase to search for and click **Go** to display the results of the search.
   - Select **Highlight search results** to highlight your search term in each of the results.
4. Click any of the search results to display the help topic.

System Configuration

This section describes the key system settings to configure or revise after you have installed the Polycom® RealPresence® Access Director™ system and entered the initial network settings (see the *RealPresence Access Director Getting Started Guide*, available at support.polycom.com).

The topics below describe configuration details and indicate the recommended order for configuring system settings:

See the *Polycom RealPresence Access Director System Getting Started Guide* (available at support.polycom.com) for information on initial installation and configuration of the system.

For deployment information, see *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*.

Configuring Time Settings

The **Time Settings** function allows you to configure time settings after the initial installation of your system and to edit the system time and time zone when necessary.

Consider the following information before changing the time settings.

- Changing the time settings requires a system restart, which terminates active calls and logs all users out of the system.

- Changing the time settings can affect the number of days available for a trial period license.
- If you plan to install an identity certificate provided by a certificate authority (CA), submit a certificate signing request to a CA server located in the same time zone as your system. If the time zones are different, or if you change the time zone after installing the CA certificate, the certificate may not be valid. If this happens, you must request and install a new certificate.

If you plan to use your system to support calls between endpoints in your enterprise and endpoints in a separate but federated (trusted) division or enterprise that has its own RealPresence Access Director system, both systems and the CA server should be in the same time zone. If the time difference between the two RealPresence Access Director systems and the CA server is too great, the TLS connection may fail.

Setting the Time Zone

After initial installation of the RealPresence Access Director system, the default time zone is GMT (UTC). After you launch the system for the first time, you must specify the time zone of your geographic location.

Polycom strongly recommends that you select the time zone of your specific geographic location, for example, America/Denver, instead of a generic GMT offset (such as GMT+7).

If you choose a generic GMT offset, the time displays with the Linux/Posix convention for specifying the number of hours ahead of or behind GMT. Therefore, the generic equivalent of America/Denver (UTC-07:00) is GMT+07, not GMT-07.

To set the time zone

1. Go to **Admin > Time Settings > System time zone**.
2. Select the time zone of your specific geographic location, for example, America/Denver, instead of a generic GMT offset (such as GMT+7).
3. Click **Update**.
4. Click **OK** to accept your settings and restart the system.

   The **Server Time (Refresh every 10 seconds)** value refreshes based on the new settings.

Editing the Time Settings

The RealPresence Access Director system displays two different time settings as described below:

- Client date and time: In the upper right corner of the **Time Settings** window, next to your user name, the system displays the date and time of your local machine. These values change only if you revise the date and time on your local machine.

- Server time: **Server Time (Refresh every 10 seconds)** indicates the server time. If you change the **System time zone** or **Manually set the system time**, the **Server Time (Refresh every 10 seconds)** field displays the correct server time.

Polycom recommends that you configure at least two Network Time Protocol (NTP) servers for maintaining system time. The NTP server addresses may be provisioned by the Polycom® RealPresence® Resource Manager system or manually entered, as described in this section.

To edit the time settings

1. Go to **Admin > Time Settings**.
2. Complete the following fields as needed for your system:

Field	Description
System time zone	The time zone in which your RealPresence Access Director system is located. **Note** After initial installation of the RealPresence Access Director system, the default time zone is Asia/Shanghai. You must select the time zone of your geographic location immediately after installation of the system.
Auto adjust for Daylight Saving Time	Automatically determined in accordance with the system time zone. If the system time zone you select observes Daylight Saving Time, this setting is enabled. **Note** The administrator cannot change this setting.
Manually set system time	**Note** Polycom strongly recommends that you do not set the time and date manually. Manually setting system time removes NTP server information and sets the manually entered time for the selected time zone instead of for the current system UTC offset.
NTP servers	The IP addresses or FQDNs of the Network Time Protocol (NTP) servers. These server addresses may be provisioned by the Polycom® RealPresence® Resource Manager system or manually entered. See the *Polycom RealPresence Access Director Deployment Guide* for additional information about NTP servers **Note** Polycom recommends that you specify at least two NTP servers for synchronizing system time.

3 Click **Update**.

If you change the **System time zone** or **Manually set the system time**, the **Server Time (Refresh every 10 seconds)** value refreshes based on the new settings.

Changing the time settings requires a system restart, which terminates active calls and logs all users out of the system.

Working with Licenses

The RealPresence Access Director system is licensed by the number of concurrent calls. When the number of SIP and H.323 concurrent calls equals the maximum number of calls allowed by the license, or concurrent media bandwidth has reached the maximum bandwidth configured on the RealPresence Access Director system, new calls are rejected.

If you deploy two RealPresence Access Director systems in a tunnel configuration, one acts as the tunnel server and the other as the tunnel client. Each system requires a separate license.

If you purchase a license that supports tunnel encryption, you can enable the tunnel encryption in the RealPresence Access Director system user interface after you obtain your activation key code and activate your license.

Each new RealPresence Access Director system comes with a trial period license for five concurrent calls, to be used within 60 days after your system was initially installed.

The system does not send notification when the 60-day trial period license is close to expiration. If you use the trial license before activating your purchased license, note the date when the trial period license expires to prevent any interruption to call services.

Obtaining an Activation Key Code

To activate the license for your RealPresence Access Director system, you must obtain an activation key code after completing the initial configuration of a new system or when updating to a major release (for example, 3.x to 4.x) or minor release (for example, 3.1 to 3.2). You do not need an activation key when updating a patch or maintenance release (for example, 3.1.1 to 3.1.2). However, you should read the product release notes for specific information about whether or not you'll need an activation key.

To request an activation key code for a major or minor software upgrade

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

2 In the **Licensing & Product Registration** section, select **Activation/Upgrade**.

3 Select **All Other Polycom Products**.

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

5 Click **SITE & Single Activation/Upgrade**.

6 Accept the **EXPORT RESTRICTION** agreement.

7 In **Product Activation**, enter the serial number of your RealPresence Access Director system server and click **Next**.

8 Click the **Upgrade** tab to view the **Upgrade Key Codes** available for your serial number.

9 Record the **Upgrade Key Code** for the software upgrade and use it to activate your license after installing the upgrade file. See Activating a License on page 23.

To request an activation key code for a new installation

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

2 Select **Licensing & Product Registration > Activation/Upgrade**.

3 Select **All other Polycom Products**.

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

5 Click **SITE & Single Activation/Upgrade**.

6 Accept the **EXPORT RESTRICTION** agreement.

7 In **Product Activation**, enter the serial number of your RealPresence Access Director system server and click **Next**.

8 Enter the license number you received for your system and click **Activate**.

The key code displays.

9 Click the **Upgrade Tab** to view any **Upgrade Key Codes** available for your serial number.

10 If an **Upgrade Key Code** is available, record the key code and use it to activate your license. See Activating a License on page 23.

Activating a License

To activate a license

1 In the RealPresence Access Director system user interface, go to **Maintenance > License**.

2 Enter the **Activation key** for the license and click **Update**.

The system restarts.

Viewing License Information

To view license information

» Go to **Maintenance > License**.

The following information displays:

Field	Description
Active License	
Licensed calls	Maximum number of calls that the license permits.
Remaining trial period	The time remaining in the trial period. Commercial licenses have no trial period limitation.
Activation Keys	
Serial number	Serial number of the RealPresence Access Director system server.
Activation key	The activation key that you received from Polycom when you provided your system's license number and serial number.

Configuring Network Settings

Many of the network settings for the RealPresence Access Director system are defined during First Time Setup but may be revised at any time. For information on configuring the initial network settings, see the *Polycom RealPresence Access Director System Getting Started Guide*.

This following topics provide detailed information about network settings:

- Network Settings Overview on page 24
- Configuring Network Settings for One Interface on page 30
- Configuring Network Settings for One or More Network Interfaces on page 30
- Configuring Static Route Settings on page 33

Changing any network settings requires a system restart, which terminates all active calls and logs all users out of the system.

If your RealPresence Access Director system uses a CA-provided identity certificate, you must update the certificate if you change the hostname (General Network Settings) or the signaling relay address (Service Network Settings).

Network Settings Overview

Always configure network settings based on how you have deployed your RealPresence Access Director system. For more information on different deployment scenarios, see *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*.

The table below describes the following:

- All network configuration settings for the RealPresence Access Director system. Fields marked with an asterisk (*) are mandatory
- When settings are configured for the first time

- Whether specific values for a setting are necessary

Element	Description	Settings
General Network Settings		
* Hostname	Hostname of the RealPresence Access Director system. Hostname must begin with a letter and contain only letters, numbers, and internal hyphens. The reserved values appserv* and dmamgk-* cannot be used for host names.	Enter after opening the user interface for the first time during initial configuration.
* Primary DNS	IP address of the primary Domain Name Server (DNS) for the network to which the system connects.	Enter after opening the user interface for the first time during initial configuration.
Secondary DNS	IP address of the secondary DNS server for the network to which the system connects.	Enter after initial configuration.
Tertiary DNS	IP address of the tertiary DNS server for the network to which the system connects.	Enter after initial configuration.
Search Domain	One or more domain names, separated by spaces. The system domain from the **Domain** field is added automatically.	Enter after initial configuration.
Domain	Domain to which the RealPresence Access Director system belongs. `<Host Name>.<Domain>`	Enter after opening the user interface for the first time during initial configuration.
Advanced Network Settings		
Mode	The mode of the network interface card.	System installation default for eth0 is **Static**. System installation default for eth1, eth2, and eth3 is **Static** if the server has more than one NIC. **DHCP** displays if you have not yet entered a static IP address.
Device	MAC address and name of the network interface card.	System installation default for eth0. System installation default for eth1, eth2, and eth3 if server has more than one NIC.

Element	Description	Settings
* IPv4 Address	IPv4 address of the RealPresence Access Director system.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. Enter for eth1, eth2, and/or eth3 after initial configuration if the RealPresence Access Director system server has more than one NIC.
* IPv4 Subnet Mask	IPv4 subnet mask of the RealPresence Access Director system's IP address.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. Enter for eth1, eth2, and/or eth3 after initial configuration if the RealPresence Access Director system server has more than one NIC.
* IPv4 Default Gateway	IP address of the gateway server used to route network traffic outside the subnet.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. Enter for eth1, eth2, and/or eth3 after initial configuration if the RealPresence Access Director system server has more than one NIC.
Service Network Settings		
SIP/H.323 Settings		
* External signaling IP	The IP address of the network interface used for SIP and H.323 signaling and access proxy traffic between the RealPresence Access Director system and external networks.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.

Element	Description	Settings
* Internal signaling IP	IP address of the network interface used for internal SIP and H.323 signaling and access proxy traffic.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.
Media Relay		
* External Relay IP	IP address of the network interface used for media relay between the RealPresence Access Director system and external networks.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.
* Internal Relay IP	IP address of the network interface used for media relay between the RealPresence Access Director system and the internal enterprise network.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.
Management IP Settings		
* Management IP	IP address of the network interface used for management traffic, including Web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.

Element	Description	Settings
Access Proxy Settings		
* External Access Proxy IP	IP address of the network interface used for access proxy traffic between the RealPresence Access Director system and external endpoints.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After initial configuration, multiple interfaces can be selected as external access proxy IP addresses if the RealPresence Access Director system server has more than one NIC.
* Internal Access Proxy IP	IP address of the network interface used for access proxy traffic between the RealPresence Access Director system and internal network application servers.	Enter for eth0 when using the **Configuration Wizard** for the first time during initial configuration. After installation, can be changed to the IP address of eth1, eth2, or eth3 if the RealPresence Access Director system server has more than one NIC.
DMZ Setting		
Deployed behind Outside Firewall/NAT	When selected, enables DMZ settings for the system. ***If the system is deployed in the DMZ of a firewall, you must select this option.*** Disable the option if the system is deployed behind an outside firewall without NAT.	Disabled after initial installation.
Signaling relay address *	Mandatory if **Deployed behind Outside Firewall/NAT** is enabled. Specifies the RealPresence Access Director system's public IP address for signaling traffic. This IP address must be mapped on the outside firewall. **Note** If you change the signaling relay address, you must create and install new certificates on the RealPresence Access Director system if the remote endpoint uses IP addresses instead of FQDNs to establish TLS connections to the system.	None after initial installation.

Element	Description	Settings
Media relay address *	Mandatory if **Deployed behind Outside Firewall/NAT** is enabled. Specifies the RealPresence Access Director system's public IP address for media traffic. This IP address must be mapped on the outside firewall.	None after initial installation.
Static Route Settings		
Available NICs	Lists the network interfaces selected in the **Service network setting** tab	Defaults to eth0 after initial configuration. If server has more than one NIC, lists eth1, eth2, and/or eth3 after selecting the values in the Service network setting tab.
Selected NICs	Lists the NICs selected from the Available NICs list. Static routes can be configured for the selected NICs.	None after initial installation.
* Network destination	The IP address of the network to which traffic is forwarded.	None after initial installation.
* Netmask	The subnet mask of the network destination.	None after initial installation.
* Gateway	The gateway through which traffic can reach the network destination. The gateway must be in the same subnet with the selected NIC.	None after initial installation.
Static route list settings table	Displays the following details for the static routes that have been configured: • Interface Name • Interface IP • Network destination • Netmask • Gateway	

Viewing Network Settings

The main Network Settings page allows you to view and configure all network and static route settings.

To view Network settings or Static route settings

1. Go to **Admin > Network Settings**.

   The **Network settings** tab displays.

2. Click the **Static route settings** tab to view static route details.

Configuring Network Settings for One Interface

When using only one network interface for the RealPresence Access Director system, configure the network settings for all external and internal signaling, media, access proxy, and management traffic for the eth0 network interface.

To configure network settings for one interface

1. Go to **Admin > Network Settings**.
2. Click **Configure Network Setting**.
3. In the **Step 1 of 3: General Network Settings** window, select or confirm the general network settings for **eth0** as described in Network Settings Overview on page 24 and click **Next**.
4. In the **Step 2 of 3: Advanced Network Settings** window, select or confirm the required settings for **eth0** as described in Network Settings Overview on page 24 and click **Next**.
5. In the **Step 3 of 3: Service Network Settings** window, select or confirm the required settings for **eth0** as described in Network Settings Overview on page 24 and click **Done**.
   - In **Access Proxy Settings**, the IP address of the eth0 interface should display in the **External Access Proxy IP** list. if it doesn't, select it from the **Available IP address** list and click the right arrow to move it to the **External Access Proxy IP** list.
6. Select **Deployed behind Outside Firewall** if the RealPresence Access Director system is deployed behind the enterprise's outside firewall/NAT. If enabled, complete the required fields:
   - **Signaling relay address**: the signaling IP address for remote clients. This address must be the public IP address of the RealPresence Access Director system mapped on the outside firewall.
   - **Media relay address**: the media IP address for remote clients. This address must be the public IP address of the RealPresence Access Director system mapped on the outside firewall.

You must create a certificate signing request to apply for a new CA certificate for the RealPresence Access Director system if:

- You revise the signaling relay address, and
- The remote endpoint uses IP addresses instead of FQDNs to establish TLS connections to the RealPresence Access Director system.

7. Click **Done > Commit** and **Reboot Now** to save your settings and restart the system.

Configuring Network Settings for One or More Network Interfaces

If you use more than one network interface on your RealPresence Access Director system, you must configure each network interface for the type of service it communicates.

Changing any network settings requires a system restart, which terminates all active calls and logs all users out of the system.

If the system uses a CA-provided identity certificate, you must update the certificate if you change host names or signaling relay address.

You can distribute the management, external signaling, internal signaling, external media, and internal media traffic in various ways based on the number of network interfaces you have configure.

The table below describes the recommended configurations for assigning communication traffic to the network interfaces.

You can assign one to four network interfaces as external access proxy IP addresses. Only one interface can be assigned as the internal access proxy IP address.

Number of Network Interfaces	eth0 IP Address	eth1 IP Address	eth2 IP Address	eth3 IP Address
1	• Management • External SIP and H.323 signaling • Internal SIP and H.323 signaling • External media • Internal media • External access proxy • Internal access proxy			
2	• Management • Internal SIP and H.323 signaling • Internal media • Internal access proxy	• External SIP and H.323 signaling • External media • External access proxy		
3	• Management	• External SIP and H.323 signaling • External media • External access proxy	• Internal SIP and H.323 signaling • Internal media • Internal access proxy	
4	• Management • Internal SIP and H.323 signaling • Internal access proxy	• External SIP and H.323 signaling • External access proxy	• External media	• Internal media

To configure more than one network interface

1 Go to **Admin > Network Settings > Configure Network Setting**.

2 In the **Step 1 of 3: General Network Settings** window, confirm the general network settings for **eth0** as described in Network Settings Overview on page 24 and click **Next**.

3 In the **Step 2 of 3: Advanced Network Settings** window, click each of the network interfaces to configure and complete the following fields as described in Network Settings Overview on page 24.

- **IPv4 Address**
- **IPv4 Subnet Mask**
- **IPv4 Default Gateway**

4 Click **Next**.

5 In the **Step 3 of 3: Service Network Settings** window, select the IP address of the network interface to assign to each type of traffic, as described in the table below (see Network Settings Overview on page 24 for field definitions):

Settings	Field
SIP/H.323	• **External signaling IP** • **Internal signaling IP**
Media Relay	• **External signaling IP** • **Internal signaling IP**
Management IP	• **Management IP**
Access Proxy	• **External Access Proxy IP** ⮝ From the **Available IP address** list, select an IP address and click the right arrow to move the IP address to the **External Access Proxy IP** list. You can select up to four interface IP addresses to act as external IP addresses for access proxy. See the chapter on *Network Interface Configurations* in *Deploying Polycom Unified Communications in RealPresence Access Director System Environments* for recommended settings based on the number of network interfaces. • **Internal Access Proxy IP**
DMZ	If **Deployed behind Outside Firewall/NAT** is enabled, complete these fields: • **Signaling relay address** • **Media relay address**

You must create a signing request to apply for a new CA certificate for the RealPresence Access Director system if:

- You revise the signaling relay address, and
- The remote endpoint uses IP addresses instead of FQDNs to establish TLS connections to the RealPresence Access Director system.

6 Click **Done > Commit and Reboot Now** to save the network settings.

Configuring Static Route Settings

Depending on how you have deployed the RealPresence Access Director system in your network, different routing policies may be applicable for different traffic destinations. Asymmetric routing issues may occur if the RealPresence Access Director system is deployed in the DMZ in a network topology that has two physical firewalls. In this case, you must define static routes for routing traffic to the correct network destination.

To prevent asymmetric routing issues, static routes can be defined for each available network interface in your system. The **Static route setting** tab displays the network interfaces you configured in the **Service network settings** and enables you to add one or more static routes for each network interface.

To add a static route for a network interface

1. Go to **Admin > Network Settings > Static route setting**.
2. From the list of **Available NICs**, select the network interface for the new static route.
3. Click the right arrow to add the network interface to the list of **Selected NICs**.
4. Enter the **Static route setting** information:
   - **Network destination**: The IP address of the network to which traffic is forwarded. For example, the IP address of the enterprise intranet.
   - **Netmask**: The subnet of the network destination.
   - **Gateway**: The gateway through which traffic can reach the network destination. The gateway must be in the same subnet with the selected NIC.
5. Click **Add**.

   The new static route for the network interface displays in the **Static Route list**.
6. Click **Update** to save the settings.

To delete a static route for a network interface

1. Go to **Admin > Network Settings > Static route setting**.
2. In the **Static Route list**, select the static route to delete.
3. Click **Delete**.
4. Click **Update**.

   The system deletes the static route and removes it from the **Static Route list**.

To remove a network interface from the Selected NICs list

1. Go to **Admin > Network Settings > Static route setting**.
2. From the list of **Selected NICs**, select the network interface to remove.
3. Click the left arrow button to move the network interface to the list of **Available NICs**.

Configuring Tunnel Settings Between Two Systems

If you deploy two RealPresence Access Director systems in a tunnel configuration, one system acts as the tunnel server and the other system as the tunnel client. In a tunnel configuration, all traffic between the tunnel server and tunnel client uses a single port on the inside firewall, thereby reducing the number of firewall ports that must be opened.

In a two-box tunnel deployment, certain IP addresses are reserved for internal system use. The IP address you define for each system must differ from the IP addresses listed below:

- Non-encrypted tunnel: 192.168.99.21
- Encrypted tunnel: 192.168.99.1 - 192.168.99.21

Each RealPresence Access Director system requires an individual license. Although each system can be licensed for a different number of calls, the system with the fewest licensed calls determines the total number of calls that can traverse the tunnel.

Before enabling the tunnel feature, activate the licenses for both of the RealPresence Access Director systems. See Working with Licenses on page 22.

If you deploy a two-box tunnel configuration, the HTTP tunnel reverse proxy feature within access proxy is not supported. If you enable the two-box tunnel configuration and then configure an HTTP tunnel reverse proxy, the two-box tunnel will automatically be disabled. Similarly, if you configure an HTTP tunnel reverse proxy, the proxy will be disabled if you then enable the two-box tunnel configuration. For information on the HTTP tunnel reverse proxy feature, see the *Polycom RealPresence Access Director System Administrator's Guide*.

The following topics describe how to configure two-box tunnel settings and the network settings for the tunnel:

- Configuring Network Settings on the Tunnel Server on page 34
- Configuring Network Settings on the Tunnel Client on page 36
- Configuring Two-box Tunnel Settings on the Tunnel Server on page 37
- Configuring Two-box Tunnel Settings on the Tunnel Client on page 38

For more information on the tunnel feature and deployment details, see *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*.

When the tunnel feature is enabled, some RealPresence Access Director system functions are enabled only on the tunnel server user interface. These functions are not required on the tunnel client and do not display in the tunnel client user interface.

Configuring Network Settings on the Tunnel Server

In a two-box tunnel deployment, most network settings are configured on the RealPresence Access Director system that will act as the tunnel server, located in the corporate back-to-back DMZ. Network settings for

the tunnel server can be configured for one to four network interfaces. Note that you must also assign a network interface for the tunnel itself. *On the tunnel server, the network interface assigned to tunnel communication is the IP address of the remote tunnel client.*

See *Deploying Polycom Unified Communications in RealPresence Access Director System Environments* for the recommended network interface configurations based on the number of network interfaces used on the tunnel server and tunnel client.

To configure network settings for the tunnel server

1. From your Web browser, enter the IP address of the RealPresence Access Director system that will act as the tunnel server and log into the user interface.
2. Go to **Admin > Network Settings > Configure Network Setting**.
3. In the **Step 1 of 3: General Network Settings** window, confirm the general network settings for **eth0** as described in Network Settings Overview on page 24 and click **Next**.
4. In the **Step 2 of 3: Advanced Network Settings** window, click each of the network interfaces to configure and complete the following fields as described in Network Settings Overview on page 24.
   - **IPv4 Address**
   - **IPv4 Subnet Mask**
   - **IPv4 Default Gateway**
5. Click **Next**.
6. In the **Step 3 of 3: Service Network Settings** window, select the IP address of the network interface to assign to each type of traffic and to the tunnel for communication between the tunnel server and tunnel client:
   - **External Signaling IP**: The IP address of the network interface used for SIP and H.323 signaling and access proxy traffic between the RealPresence Access Director system and external networks.
   - **External Relay IP:** The IP address of the network interface used for media relay between the RealPresence Access Director system and external networks.
   - **Management IP:** The IP address of the network interface used for communication between the tunnel server and tunnel client and management traffic, including Web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.
     - If you are using three or four network interfaces on the tunnel server, tunnel communication between the two systems and management traffic may be assigned to different network interfaces. In this case, select the network interface used for management traffic in the **Management IP** field. Configure the interface for tunnel communication between the two systems in the Two-box Tunnel Settings (see Configuring Two-box Tunnel Settings on the Tunnel Server on page 37). On the tunnel server, the network interface assigned to tunnel communication between the two systems is the IP address of the remote tunnel client.
   - **External Access Proxy IP**: From the **Available IP address** list, select a network interface to assign as an external access proxy IP address and click the right arrow to move it to the **External Access Proxy IP** list. You can assign up to four external access proxy IP addresses.

7 Select **Deployed behind Outside Firewall/NAT** and enter the following information:

- **Signaling relay address**: The RealPresence Access Director system's public IP address for signaling traffic. This IP address must be mapped on the outside firewall.
- **Media relay address**: The RealPresence Access Director system's public IP address for media traffic. This IP address must be mapped on the outside firewall.

Depending on your network interface configuration, the Signaling relay address and the Media relay address may be the same IP address.

8 Click **Done > Commit and Reboot Now** to save the network settings.

Configuring Network Settings on the Tunnel Client

Network settings for the tunnel client can be configured for one to three network interfaces. *On the tunnel client, the network interface assigned to tunnel communication is the IP address of the remote tunnel server.*

To configure network settings for the tunnel client

1 From your Web browser, enter the IP address of the RealPresence Access Director system that will act as the tunnel client and log into the user interface.

2 Go to **Admin > Network Settings > Configure Network Setting**.

3 In the **Step 1 of 3: General Network Settings** window, confirm the general network settings for **eth0** as described in Network Settings Overview on page 24 and click **Next**.

The **General Network Settings** that display are the settings configured for eth0 during initial installation and first-time setup of the system.

4 In the **Step 2 of 3: Advanced Network Settings** window, click each of the network interfaces to configure and complete the following fields as described in Network Settings Overview on page 24.

- **IPv4 Address**
- **IPv4 Subnet Mask**
- **IPv4 Default Gateway**

5 Click **Next**.

6 In the **Step 3 of 3: Service Network Settings** window, select the network interface to assign as the **Management IP** address. The network interface that handles management traffic is based on the number of network interfaces configured on the tunnel client. See the *Network Interface Configurations* chapter in *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*.

7 Click **Done > Commit and Reboot Now** to save the network settings.

If the tunnel client uses more than one network interface, go to **Configure > Tunnel Settings** to specify the IP address of the network interface that the tunnel client uses for internal signaling and media communication with the RealPresence DMA system. See the **Internal signaling/media/access proxy IP of tunnel client** field in Configuring Two-box Tunnel Settings on the Tunnel Client on page 38.

Configuring Two-box Tunnel Settings on the Tunnel Server

If you use the encryption option for the two-box tunnel, you must first synchronize the time on the tunnel server and the tunnel client to the same Network Time Protocol (NTP) server *before* encrypting the tunnel. See *Deploying Polycom Unified Communications in RealPresence Access Director System Environments* for additional details and refer to Configuring Time Settings on page 19.

Due to legal requirements in some countries related to the encryption of data, the option to encrypt the two-box tunnel is not available in all instances of the RealPresence Access Director system.

To configure settings on the tunnel server

1. Go to **Configuration > Two-box Tunnel Settings**.
2. Use the information in the table below to configure the settings for your system. An asterisk (*) indicates a required field.

Field	Description
Enable Tunnel	Select to enable the two-box tunnel feature.
Settings	
Server Client	Select **Server** to enable the system to operate as a tunnel server.
Encrypted tunnel	When selected, communications between the tunnel server and tunnel client are encrypted. **Note** • This option displays only if you purchase a license that supports encryption of the tunnel between two systems. If supported, select this option to encrypt the tunnel after you obtain your activation key code and activate your license. • ***This setting must be the same on both the tunnel server and tunnel client.***
* Local tunnel server address	The IP address and port number of the tunnel server. Default port: 1194 **Note** Polycom recommends that you use the default port number 1194, but you can use any value from 1190-1199 or 65380-65389.
* Remote tunnel client address	The IP address and port number of the tunnel client. Default port: 1194
* Internal signaling/media/access proxy IP of tunnel client	The IP address of the network interface that the tunnel client uses for internal signaling, internal media, and internal access proxy communication with the RealPresence DMA system.

3 Click **Update**.

The system restarts.

Configuring Two-box Tunnel Settings on the Tunnel Client

When configuring settings on the tunnel client, ensure that the time on the tunnel server and the tunnel client has been synchronized to the same NTP server *before* encrypting the tunnel. See Configuring Two-box Tunnel Settings on the Tunnel Server on page 37.

To configure two-box tunnel settings on the tunnel client

1 Go to **Configuration > Two-box Tunnel Settings**.

2 Use the information in the table below to configure the settings for your system. An asterisk (*) indicates a required field.

Field	Description
Enable Tunnel	The tunnel feature is enabled if you have configured the tunnel server.
Settings	
Server Client	Select **Client** to enable the system to operate as the tunnel client.
Encrypted tunnel	When selected, tunnel communications are encrypted. **Note** • This option displays only if you purchase a license that supports encryption of the tunnel between two systems. If supported, select this option to encrypt the tunnel after you obtain your activation key code and activate your license. • ***This setting must be the same on both the tunnel server and tunnel client.***
* Local tunnel client address	The IP address and port number of the tunnel client. Default port: 1194 **Note** Polycom recommends that you use the default port number 1194, but you can use any value from 1190-1199 or 65380-65389.
* Remote tunnel server address	The IP address and port number of the tunnel server. Default port: 1194
* Internal signaling/media/access proxy IP of tunnel client	The IP address of the network interface that the tunnel client uses for internal signaling, internal media, and internal access proxy communication with the RealPresence DMA system.

3 Click **Update**.

The system restarts.

The two-box tunnel connection status displays on the user interface Dashboard on both the tunnel server and tunnel client.

Working with Certificates

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other. X.509 certificates enhance security based on the following:

- A single, centralized certificate authority (CA) is established. Typically, this is either an enterprise's IT department or a commercial certificate authority.
- Each computer on the network is configured to trust the central certificate authority.
- Each server on the network has a public certificate that identifies the server.
- The certificate authority signs the public certificates of those servers that clients should trust.
- When a client connects to the server, the server shows its signed public certificate to the client. Trust is established because the certificate has been signed by the certificate authority, and the client has been configured to trust the certificate authority.

See the following topics for detailed information on use of certificates in the RealPresence Access Director system.

How Certificates are Used

The RealPresence Access Director system uses X.509 certificates in different ways.

- When a user logs into the RealPresence Access Director system's browser-based user interface, the RealPresence Access Director system offers an X.509 certificate to identify itself to the browser client.

  - The RealPresence Access Director system's certificate must have been signed by a certificate authority.
  - The browser must be configured to trust that certificate authority (beyond the scope of this documentation).

- When a client sets up an HTTPS, LDAP, or XMPP connection with access proxy, the RealPresence Access Director system offers an X.509 certificate to identify itself'.
- When a client sends SIP messages with TLS transport, the RealPresence Access Director system offers an X.509 certificate to identify itself.
- When the RealPresence Access Director system connects to a RealPresence Resource Manager server, the RealPresence Access Director system may present a certificate to the server to identify itself.
- When the RealPresence Access Director system connects to an ACME Packet session border controller (SBC) or to another RealPresence Access Director system for a SIP enterprise-to-enterprise call, the RealPresence Access Director system presents its certificate to the server to identify itself.

When you deploy the RealPresence Access Director system, you should apply for the TLS/SSL certificate and CA root certificate from a certificate authority for the RealPresence Access Director, RealPresence Resource Manager, and RealPresence DMA systems, and install the CA certificates on each client.

Accepted Forms of Certificates

X.509 certificates come in several forms (encoding and protocol). The following table shows the forms that can be installed on the RealPresence Access Director system.

Encoding	Protocol / File Type	Description and Installation Method
PEM (Base64-encoded ASCII text)	PKCS #7 protocol P7B file	A certificate chain containing: • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Intermediate certificates (optional). **Note** Upload the file or paste into text box.
	CER (single certificate) file	A signed certificate for the system, authenticating its public key. **Note** Upload file or paste into text box.

Encoding	Protocol / File Type	Description and Installation Method
DER (binary format using ASN.1 Distinguished Encoding Rules)	PKCS #7 protocol P7B file	A certificate chain containing: • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Intermediate certificates (optional). **Note** Upload the file.
	CER (single certificate) file	A signed certificate for the system, authenticating its public key. **Note** Upload the file.

Certificate Procedures

Certificate procedures include the following:

- Install your chosen certificate authority's public certificate, if necessary, so that the RealPresence Access Director system trusts that certificate authority.
- Create a certificate signing request to submit to the certificate authority.
- Install the public certificate signed by your certificate authority that identifies the RealPresence Access Director system.
- Remove a signed certificate or a certificate authority's certificate.

If you have two systems deployed in a tunnel configuration, the tunnel connection between the tunnel server and client uses a default self-signed certificate dedicated for tunnel use. This certificate cannot be changed but can be refreshed when it expires.

Viewing Installed Certificates

To view installed certificates

» Go to **Admin > Certificates**.

The table below describes the certificate information that displays.

Field	Description
Enable OCSP	Enables the use of Online Certificate Status Protocol to obtain the revocation status of an X.509 digital certificate presented to the system. When enabled, the system checks the certificate's AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder: • If there is none, the certificate fails validation. • Otherwise, the system sends the OCSP request to the responder identified in the certificate.
Store OCSP configuration	Saves the OCSP configuration (enabled or disabled).
Identifier	Common name of the certificate.
Cert Type	KEY_STORE contains the signed certificate that identifies the RealPresence Access Director system. TRUSTED_STORE contains trusted certificates, such as CA certificates.
Purpose	The purpose of the certificate for the RealPresence Access Director system. Server SSL is the public certificate that identifies the RealPresence Access Director system. By default, this is a self-signed certificate, not trusted by other devices. Only one Server SSL certificate can exist in the system at one time; adding a new Server SSL certificate will replace the old one. CA is the root certificate of the certificate authority that the RealPresence Access Director system trusts. The system will treat the trusted self-signed certificates from peers as CA certificates.
Valid Period	The time range during which the certificate is valid.
Refresh Certificate	Replaces the current certificate with a new self-signed certificate and restarts the RealPresence Access Director system.

Viewing Certificate Details

To view detailed information about certificates

1. Go to **Admin > Certificates**.
2. Select the certificate to view and click **Display Details**.

   Certificate Details displays the following information:

Section	Description
Certificate Info	
Purpose	The purpose of the certificate for the RealPresence Access Director system. • Server SSL is the public certificate that identifies the RealPresence Access Director system. By default, this is a self-signed certificate, not trusted by other devices. Only one Server SSL certificate can exist in the system at one time; adding a new Server SSL certificate will replace the old one. • CA is the root certificate of the Certificate Authority that the RealPresence Access Director system trusts. The system will handle the trusted self-signed certificates from peers as CA certificates.
Key usage	Indicates the operations that can be performed using the public key contained in the certificate.
Extended key usage	Indicates the purpose of the public key contained in the certificate. It contains a list of OIDs, each of which indicates an allowed use.
Issued To	
Common Name (CN)	For a Server SSL certificate, the fully qualified domain name (FQDN) of the system's management interface, as defined in the **Hostname** and **Domain** fields in **Admin > Network Settings > General Network Setting**. For a CA certificate, the common name of that certificate.
Organization (O)	Usually, the legal name of your enterprise.
Organizational unit (OU)	Subdivisions of your organization, such as Human Resources or IT, that are handling the certificate.
Serial number	The certificate serial number.
Issued By	
Common Name (CN)	The common name of the entity that issued the certificate.
Organization (O)	The name of the entity that issued the certificate.
Organizational unit (OU)	Subdivisions of the entity that issued the certificate
Validity	
Valid start date	The date the certificate was issued.
Valid end date	The date the certificate expires.
Fingerprints	
SHA-1 fingerprint	The secure hash algorithm used to confirm the certificate.
MD5 fingerprint	The message-digest algorithm used to confirm the certificate.

To Use the Online Certificate Status Protocol (OCSP)

1. Select **Enable OCSP**.
2. Click **Store OCSP configuration**.

   A **Confirm Action** dialog box displays, notifying you of two possibilities:

   - Access proxy restarts if you click **Yes** to save the configuration. This does not require a restart of the entire system.
   - The application will be restarted if you click **Yes** to save the configuration. Restarting the system is necessary if you save an OCSP configuration while SIP service is enabled.

   The system automatically displays the correct **Confirm Action** dialog box.

Adding a Certificate Authority's Public Certificate

Use this procedure to add a trusted certificate authority, either an in-house or commercial CA.

To add a certificate for a trusted root CA

1. Go to **Admin > Certificates**.

   The installed certificates are listed. The CA entries, if any, represent the certificate authorities whose public certificates are already installed on the RealPresence Access Director system and are trusted.
2. If you're using a certificate authority that isn't listed, access the certificate authority of your choice and obtain a copy of the CA's public certificate.

   The certificate must be either a single certificate or certificate chain. If it's ASCII text, it's in PEM format, and starts with the text `-----BEGIN CERTIFICATE-----`. If it's a file, it can be either PEM or DER encoded.
3. Go to **Admin > Certificates > Add Certificates**.
4. In the **Add Certificates** dialog box, do one of the following:

   - If you have a file, click **Upload certificate** 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.
5. Click **OK**.
6. In the **Confirm Action** dialog box, click **OK** to restart the system.

   The installed CA certificate is added to the TRUSTED_STORE list. There can be multiple CA certificates in the TRUSTED_STORE list.

Self-signed TLS/SSL peer certificates will be treated as CA certificates when importing them into the RealPresence Access Director system.

Creating a Certificate Signing Request

After initial installation, the RealPresence Access Director system is configured to use a self-signed certificate with an ISO file. You can create a certificate signing request (CSR) to apply for a signed certificate from a certificate authority to replace the self-signed certificate. The signed certificate identifies the RealPresence Access Director system as a trusted entity.

If you make B2B calls from your RealPresence Access Director system to another RealPresence Access Director system, both systems must have CA certificates installed. Before submitting the CSR for each system, ensure that the correct time and time zone are configured on each RealPresence Access Director system and that you submit the CSR for each system to a CA within the same time zone.

If you have two RealPresence Access Director systems deployed in a tunnel configuration, the connection between the tunnel server and tunnel client uses a default self-signed certificate dedicated for tunnel use. This certificate cannot be changed or replaced but can be refreshed when it expires.

When creating a CSR, you can specify up to 20 Subject Alternative Names (SANs). Each SAN can be an IP address or FQDNs to include on a single certificate.

If you configure access proxy settings for HTTPS proxies and specify next hops using the Host header filter, you must add the host FQDNs as Subject Alternative Names in the certificate signing request.

To create a certificate signing request

1. Go to **Admin > Certificates > Create Certificate Signing Request**.

   If a signing request has already been created, the system asks if you want to use the existing request or generate a new one. Click **Generate New** to generate a new request.

2. In the **Certificate Information** dialog box, enter the identifying information for your RealPresence Access Director system:

Field	Description
* Common Name (CN)	Defaults to the fully qualified domain name (FQDN) of the RealPresence Access Director system's management interface, as specified in **Admin > Network Settings**.
Domain	The domain name of the RealPresence Access Director system.

Field	Description
SAN List (0<=size<=20)	Optional Subject Alternative Names, which can be IPv4 addresses or FQDNs. Specifying SANs in the CSR allows additional IP addresses and/or FQDNs to be protected with just one certificate. If you create HTTPS reverse proxy next hops using the Host header filter (e.g., for the Polycom® RealPresence® CloudAXIS™ Suite Services Portal or Experiences Portal), you must specify the host FQDNs as SANs. See Configuring HTTPS Proxy Settings on page 56. To add a SAN, click the **+** (plus) icon and enter the IPv4 address or FQDN. To delete a SAN, select it and click the **X** (delete) icon. Up to 20 SANs can be specified in the certificate signing request. **Note** Each time you add or revise a Subject Alternative Name, you must submit a new CSR.
Organizational unit (OU)	The subdivision of your organization, such as Human Resources or IT, that is handling the certificate.
Organization (O)	Typically, the legal name of your enterprise.
City or locality (L)	The city where your enterprise is located.
State (ST)	The state where your enterprise is located.
* Country (C)	Two-character ISO code for the country in which your enterprise is located. Current ISO country codes

3 Click **OK**.

4 From the **Certificate Signing Request** dialog box, select and copy the entire contents of the **Encoded Request** box. Be sure to include the text:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

and

```
-----END NEW CERTIFICATE REQUEST-----
```

5 Submit the CSR.

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

The RealPresence Access Director system may act as both a server or client. When you complete the certificate signing request, be sure to specify that the Enhanced Key Usage of the certificate must indicate both Server Authentication and Client Authentication. Both Server and Client Authentication are mandatory to enable a mutual TLS connection between two session border controllers.

Key Usage must include Digital Signature and Key Encipherment.

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

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

The RealPresence Access Director system accepts PKCS#7 certificate chains.

Reviewing a Certificate

After you have submitted a certificate signing request and received the signed certificate or certificate chain from the certificate authority, you must review the certificate to ensure it is valid before adding it to the RealPresence Access Director system.

When you submit a CSR to your CA, the CA may modify the Key Usage or Enhanced/Extended Key Usage fields in the certificate. Changes to these fields invalidate the certificate and may prevent you from accessing the RealPresence Access Director system from your browser.

If you attempt to install an invalid certificate, the system displays error messages that explain why the certificate is invalid. Contact Polycom technical support (support.polycom.com) if you think an invalid certificate has been installed on your system.

To review the certificate

1 Check the following certificate details:

Certificate Field	Required Information
Valid from/Valid to	Check the validity period of the certificate to ensure that it is not expired and is currently valid. **Note** Ensure the certificate is valid for the selected time zone.
Key Usage (OID: 2.5.29.15)	DigitalSignature Key_Encipherment
Enhanced/Extended Key Usage (OID: 2.5.29.37)	Server Authentication OID: 1.3.6.1.5.5.7.3.1 Client Authentication OID: 1.3.6.1.5.5.7.3.2 Both Server Authentication and Client Authentication are mandatory for establishing a mutual TLS connection between two session border controllers.

If the required information for the certificate is missing or inaccurate, you must create a new certificate signing request and apply for a new certificate from the CA.

Adding a Signed Certificate

After you have submitted a certificate signing request and received and reviewed the signed certificate or certificate chain from the certificate authority, you can install the certificate or certificate chain in two ways:

- Upload a PEM or DER certificate file.
- Paste PEM certificate text into the text area.

Installing, replacing, and deleting certificates require a system restart, which terminates active calls and logs all users out of the system. The certificate store is updated immediately; however, the RealPresence Access Director system does not implement the update until you restart the system.

If necessary, you can delay an immediate change, enabling you to perform multiple procedures before restarting the system and applying the changes.

If you attempt to install an invalid certificate, the system will display error messages that explain why the certificate is invalid.

The table below describes the potential error messages.

Cause of Error	Error Message
Certificate is not yet valid	Current RPAD System time (example): 2000-10-10 00:12:50 CST The certificate is not yet valid. Please check valid date from and to in your certificate.
Certificate has expired	Current RPAD System time (example): 2019-10-10 00:00:39 CST The certificate has expired. Please check valid date from and to in your certificate.
Key usage of the certificate is incorrect	The key usage of the certificate should include at least DigitalSignature and Key_Encipherment.
Enhanced/Extended key usage of the certificate is incorrect	The enhanced/extended key usage of the certificate should include at least Server Authentication (1.3.6.1.5.5.7.3.1) and Client Authentication (1.3.6.1.5.5.7.3.2)

To add a signed certificate that identifies the RealPresence Access Director system

1. Go to **Admin > Certificates > Add Certificates**.
2. In the **Add Certificates** dialog box, do one of the following:

- If you have a PEM or DEM certificate file, click **Upload certificate** and browse to the file or enter the path and file name.
- If you have PEM-format text, copy the certificate text, click **Paste certificate**, and paste it into the text box below. You can paste multiple PEM certificates one after the other.

3. Click **OK**.
4. In the **Confirm Action** dialog box, click **OK** to restart the system.

   The installed certificate is added to the KEY_STORE. Only one signed certificate can be installed in the RealPresence Access Director system.

Refreshing a Signed Certificate

The KEY_STORE certificate can be renewed before it expires.

To renew the KEY_STORE certificate

1. Go to **Admin > Certificates**.
2. Select the KEY_STORE certificate and click **Refresh**.

   The certificate is renewed for one year.

Replacing a Signed Certificate

To replace a signed certificate

1. Complete the signing request procedure described in To create a certificate signing request on page 45.
2. Access a certificate authority and use the text from the certificate signing request to apply for a certificate.
3. Download the certificate or certificate chain.
4. Go to **Admin > Certificates > Add Certificates**.
5. Upload the certificate file or paste the text from the certificate file.

   See Adding a Signed Certificate on page 48
6. Click **OK**.
7. In the **Confirm Action** dialog box, click **OK** to restart the system.

The signed certificate replaces the previously installed signed certificate in the KEY_STORE.

Deleting Certificates

In the RealPresence Access Director system, you can delete certain certificates.

To delete a certificate

1. Go to **Admin > Certificates**.
2. Select the certificate to delete.

   If the certificate is eligible for deletion, **Delete Certificate** displays under **Actions**.

The RealPresence Access Director system Server SSL certificate and the last CA certificate cannot be deleted. If you select either of these certificates, the **Delete Certificate** option does not display.

3. Click **Delete Certificate**.
4. In the **Information** dialog box, click **OK**.
5. In the **Confirm Action** dialog box, click **Yes** to restart the system.

Provisioning the System

When the RealPresence Access Director system is integrated with a Polycom RealPresence Resource Manager system, the RealPresence Resource Manager system can provision some of the settings for the RealPresence Access Director system. Additionally, the RealPresence Access Director system supports provisioning of remote endpoints if the endpoints are registered with the RealPresence Resource Manager system. For details on endpoint provisioning, see the *Polycom RealPresence Resource Manager System Operations Guide* for your version of the RealPresence Resource Manager system.

Provisioning of the RealPresence Access Director system is optional. If not provisioned, you must manually configure all system settings.

The table below describes the settings that the RealPresence Resource Manager system can provision for the RealPresence Access Director system.

Field	Description
Time Server	Configures whether the RealPresence Access Director system uses a time server to synchronize system time.
Primary Time Server Address	The IP address of the primary time server that the system will use to synchronize time.
Secondary Time Server Address	The IP address of the secondary time server that the system will use to synchronize time.
Enable IP H.323	Configures the system to enable or disable H.323 signal forwarding.
Gatekeeper Address	The IP address of the internal gatekeeper that the system forwards to when endpoints behind the system send gatekeeper registration or H.323 call requests.
Enable SIP	Configures the system to enable or disable SIP signal forwarding.

Field	Description
Proxy Server	The IP address of the internal SIP proxy server that the system forwards to when endpoints behind the system send SIP call requests.
Registrar Server	The IP address of the internal SIP registrar server that the system forwards to when endpoints behind the system send SIP registration requests.
Transport Protocol	The protocol the system uses for SIP signaling.

Connecting to the Polycom Management System

To enable provisioning, the RealPresence Access Director system must have a user account with the RealPresence Resource Manager system. When you log into the user account from the RealPresence Access Director system user interface, the RealPresence Resource Manager system can provision your system.

For information about configuring the RealPresence Resource Manager system to provision the RealPresence Access Director system, refer to *Unified Communications with the Polycom RealPresence Access Director System Solutions*.

To connect to the RealPresence Resource Manager system for provisioning

1. Go to **Admin > Polycom Management System**.
2. Enter the required log-in information and the RealPresence Resource Manager system IP address.

Field	Description
Login Name	The name of the RealPresence Access Director system user account.
Password	The password of the RealPresence Access Director system user account.
Address	The IP address of the RealPresence Resource Manager system.
Verify certificate from internal server	Enable if certificates need to be verified between the RealPresence Access Director system and the RealPresence Resource Manager system. **Note** Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence Access Director system and the RealPresence Resource Manager system.

3. Click **Connect**.

   The RealPresence Resource Manager system provisions the settings for the RealPresence Access Director system.

To disconnect from the RealPresence Resource Manager System

1. Go to **Admin > Polycom Management System**.
2. Click **Disconnect**.

Integrating with Microsoft Active Directory

The RealPresence Access Director system integrates with Microsoft® Active Directory® to enable user authentication. This integration provides two key benefits:

- Allows Active Directory users to log into the RealPresence Access Director system by entering their Active Directory credentials.
- Enables you to map roles to Active Directory groups rather than to individual users.

The RealPresence Access Director system supports one Active Directory domain and does not support sub domains.

To integrate with Active Directory

1. Go to **Admin > Microsoft Active Directory**.
2. Select **Enable integration with Microsoft Active Directory Server**.
3. Complete the following fields as needed for your system:

Field	Description
Directory server address	The IP address or FQDN of the Active Directory server.
Domain\User name	The domain and user name that the RealPresence Access Director system uses to log into Active Directory and retrieve domain and group information.
Password	The password that the RealPresence Access Director system uses to log into Active Directory.
Base DN	Optional. Base distinguished name (DN) is the top level of the LDAP directory. Specify the base DN in the following form (case insensitive): `DC=Polycom,DC=com` The RealPresence Access Director system fetches Active Directory domains from the specified base DN.

Field	Description
Security level	The security level for the connection and communication between the RealPresence Access Director system and the Active Directory server. Three options are available: • **Plain**: Uses the LDAPv2 extension; all communication between the RealPresence Access Director system and the Active Directory server is in plain text (low security). • **LDAPS**: Also known as LDAP over SSL; uses the LDAPv2 extension (medium security). ▲ If you select this level of security, do not enable **Verify certificate from internal server**. • **StartTLS**: Uses the LDAPv3 extension to establish a TLS connection over the existing LDAP connection with the Active Directory server. (high security). Polycom recommends selecting **StartTLS** for the most secure LDAP communication.
Verify certificate from internal server	When selected, the RealPresence Access Director system validates the Active Directory certificate when establishing a connection with Active Directory.

4 Click **Update**.

Using Role Mapping Settings

To add a group and assign a mapping role

1 Go to **Admin > Microsoft Active Directory**.

2 Ensure that **Enable integration with Microsoft Active Directory Server** is selected.

3 Click **Add** and provide the following information:

- **Group name in Active Directory**: Enter the name of the Active Directory group. A name can include letters, numbers and the dash (**-**), underscore (**_**), and backward slash (****) special characters
- **Mapping Role**: Select the role to assign to the Active Directory group.

To view the Active Directory groups, access the Active Directory server. Note the names of the groups for which you will map roles in the RealPresence Access Director system.

4 Click **OK**.

5 Click **Update**.

To edit the role of an Active Directory group

1. Go to **Admin > Microsoft Active Directory**.
2. Ensure that **Enable integration with Microsoft Active Directory Server** is selected.
3. In the **Role Mapping Setting** table, select the group and click **Edit**.
4. In **Mapping Role**, select a different role as needed.
5. Click **OK**.
6. Click **Update**.

To delete an Active Directory group

1. Go to **Admin > Microsoft Active Directory**.
2. Ensure that **Enable integration with Microsoft Active Directory Server** is selected.
3. In the **Role Mapping Setting** table, select the group and click **Delete**.
4. In the **Confirm Action** window, click **OK**.
5. Click **Update**.

Working with Access Proxy Settings

The access proxy feature in the RealPresence Access Director system provides reverse proxy services for external client endpoints. You can configure reverse proxies to enable firewall/NAT traversal for various types of connections. When access proxy receives a request from an external client, the RealPresence Access Director system accepts the request and sends a new request on behalf of the client to the appropriate application server.

The RealPresence Access Director system is configured with three default reverse proxies that route communication requests based on the type of target application server:

- **HTTPS_proxy**: HTTPS servers that provide management services (Polycom® RealPresence® Resource Manager system, Polycom® RealPresence® Content Sharing Suite), RealPresence CloudAXIS Suite services, and other HTTPS application servers
- **LDAP_proxy**: LDAP servers that provide directory services
- **XMPP_proxy**: XMPP servers that provide message, presence, or other XMPP services

In addition to the default proxies, the RealPresence Access Director system supports the following reverse proxy configurations:

- **PassThrough_proxy**: A passthrough reverse proxy configuration provides transparent relay of communication requests through the RealPresence Access Director system to internal application servers. Passthrough reverse proxy is used primarily for backwards compatibility with the TCP reverse proxy feature.

The **PassThrough_proxy** will not display on the main Access Proxy Settings page if you did not configure a TCP reverse proxy in a previous version of the RealPresence Access Director system.

- **HTTP tunnel proxy**: This type of proxy specifically supports SIP signaling and media relay for SIP guest calls from RealPresence CloudAXIS Suite clients to a CloudAXIS Suite Services Portal or Experience Portal server

The default proxies may be edited or you can add new proxies for various internal application servers. When you configure the proxies, you must specify an external IP address for access proxy and an external listening port. Based on the network settings you configured (see Configuring Network Settings for One or More Network Interfaces on page 30), you may have up to four external IP addresses to use for access proxy. ***You can reuse an external IP address but the port must be unique for each proxy configuration that uses the same external IP address.*** For example, if you create two proxy configurations for LDAP directory services, the combined external IP address for access proxy and the external listening port cannot be the same for both LDAP proxy configurations.

The examples below show some possible external IP address and port combinations.

Example 1

Name of Proxy	External IP Address for Access Proxy	External Listening Port
ldap_proxy_1	172.20.102.58	389
ldap_proxy_2	172.20.102.58	9980

Example 2

Name of Proxy	External IP Address for Access Proxy	External Listening Port
ldap_proxy_1	172.20.102.58	389
ldap_proxy_2	172.20.102.60	389

From the main Access Proxy Settings page, you can add new proxy configurations, edit the default proxies, and delete proxy configurations. When adding or editing proxy settings, the system validates the settings to ensure that no conflicts exist with any other reverse proxy configurations. The system displays a warning message if conflicts are found.

Before configuring any access proxy settings, you must configure the network interface settings for external and internal access proxy IP addresses. See Access Proxy Settings on page 28 for details.

Adding a New Proxy Configuration

Adding a new proxy configuration consists of selecting the protocol for the proxy and configuring the detailed settings.

To add a proxy configuration

1. Go to **Configuration > Access Proxy Settings**.
2. Under **Actions**, click **Add**.
3. In the **Step 1 of 2: Protocol Selection** window, select the **Protocol** for the new proxy and click **Next**.
4. In the **Step 2 of 2: Detailed Settings** window, configure the settings for the specific protocol of the proxy.

See the following topics for instructions on configuring the detailed proxy settings for the different protocols:

- Configuring HTTPS Proxy Settings on page 56
- Configuring LDAP Proxy Settings on page 59
- Configuring XMPP Proxy Settings on page 60
- Understanding Passthrough Proxy on page 61
- Configuring HTTP Tunnel Settings on page 62

Configuring HTTPS Proxy Settings

The access proxy feature enables external endpoints to access different internal HTTPS servers. The RealPresence Access Director system forwards HTTPS requests to the correct application server based on the HTTPS reverse proxy settings you configure.

When the RealPresence Access Director system is integrated with a Polycom RealPresence Resource Manager system, access proxy enables remote endpoints to be provisioned and managed by the RealPresence Resource Manager system. When the RealPresence Access Director system receives a log-in and provisioning request from an external endpoint, it sends the request to the HTTPS provisioning server configured within the RealPresence Resource Manager system.

Multiple HTTPS next hops can be added to an HTTPS reverse proxy configuration. For each next hop, you must apply a filter that's based on the HTTPS request message header received from the endpoint. The RealPresence Access Director system uses the filter and other settings to send the connection request to the correct internal HTTPS application server. Two filters are available:

- Request-URI: The next hop is based on the Request-URI in the message header received from the endpoint. Use the Request-URI filter only when adding a next hop to a Polycom RealPresence Resource Manager system or a Polycom RealPresence Content Sharing Suite system.
- Host header: The next hop filter is based on the host information in the message header received from the endpoint. Use a host header filter when creating the next hop for various HTTPS application servers, including the RealPresence CloudAXIS Suite Services Portal and Experience Portal.

If you add host header next hops, you must specify the host FQDNs as Subject Alternative Names (SANs) in the Certificate Signing Request for the RealPresence Access Director system. See Creating a Certificate Signing Request on page 45.

To configure HTTPS proxy settings

1. Go to **Configuration > Access Proxy Settings**.
2. Under **Actions**, click **Add**.
3. In the **Step 1 of 2: Protocol Selection** window, select **HTTPS** from the **Protocol** list and click **Next**.
4. In the **Step 2 of 2: Detailed Settings** window, complete the fields according to the table below:

Setting	Description
Name	The unique name of this HTTPS proxy configuration
External IP address	The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.
External listening port	The external port at which the RealPresence Access Director system listens for HTTPS proxy traffic. Default **HTTPS_proxy** port: 443 Range: 9980-9999 **Note** * Port 65100 is open and listening to support the access proxy process. The RealPresence Access Director system automatically redirects connections on port 443 to port 65100 to enable access proxy to function without root ownership of the process within the CentOS operating system.
Internal IP address	The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards HTTPS requests from this IP address to the requested application server.
Require client certificate from the remote endpoint	When selected, access proxy requests and verifies the client certificate from the remote endpoint.
Verify certificate from internal server	When selected, access proxy verifies the certificate from the internal HTTPS server (the RealPresence Resource Manager system or the RealPresence Content Sharing Suite).

5. Add the **Next hops**. See To add a next hop based on the Request-URI filter on page 57 and To add a next hop based on the Host header filter on page 58.

To add a next hop based on the Request-URI filter

1. Under **Next hops**, click **Add**.
2. Configure the settings as described in the table below:

Setting	Description
Type	Request-URI
Name	The unique name of this next hop
System	Polycom Management System or Polycom Content Sharing Suite **Note** Add a separate Request-URI next hop if you need to configure HTTPS settings for both systems.
Address	The internal IP address of the HTTPS server with which the remote client requested a connection. After accepting the HTTPS request from the remote endpoint, the RealPresence Access Director system sends a new HTTPS request to this IP address.
Port	The listening port of the internal HTTPS server.

3. Click **OK** to save the configuration.
4. Repeat the steps to add additional next hops as needed.

To add a next hop based on the Host header filter

1. Under **Next hops**, click **Add**.
2. Configure the settings as described in the table below:

Setting	Description
Type	Host header
Name	The unique name of this next hop
Host value	The host name in the request message header
Address	The internal IP address of the application server with which the external client has requested a connection. After accepting the HTTPS request from the external endpoint, the RealPresence Access Director system sends a new HTTPS request to this IP address.
Port	The listening port of the internal application server.

3. Click **OK** to save the configuration.

If you have more than one next hop for the same type of service, for example, two next hops for different RealPresence Resource Manager systems, you can prioritize which system the RealPresence Access Director system first contacts when routing provisioning requests.

To prioritize next hops

1. In the **Step 2 of 2: Detailed Settings** window, select a next hop.
2. Click **Priority Up** and **Priority Down** as needed to prioritize the next hops.
3. Click **Done**.
4. In the **Confirm Action** dialog box, click **Yes** to restart access proxy.

To edit an HTTPS next hop

1. In the **Step 2 of 2: Detailed Settings** window, select the next hop to revise and click **Edit**.
2. Revise the next hop settings as needed.
3. Click **OK** and then click **Done**.
4. Click **OK** to confirm the changes and restart access proxy.

To delete an HTTPS next hop

1. In the **Step 2 of 2: Detailed Settings** window, select the next hop to delete and click **Delete**.
2. Click **Done** and then **OK** to confirm the changes and restart access proxy.

Configuring LDAP Proxy Settings

LDAP reverse proxy configurations can be added to access different LDAP directory servers, such as the RealPresence Resource Manager system LDAP server or an Active Directory server.

To configure LDAP proxy settings

1. Go to **Configuration > Access Proxy Settings**.
2. Under **Actions**, click **Add**.
3. In the **Step 1 of 2: Protocol Selection** window, select **LDAP** from the **Protocol** list and click **Next**.
4. In the **Step 2 of 2: Detailed Settings** window, complete the fields according to the table below:

Setting	Description
Name	The unique name of this LDAP proxy configuration
External IP address	The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.

Setting	Description
External listening port	The external port at which the RealPresence Access Director system listens for LDAP traffic. Default **LDAP_proxy** port 389 Port range: 9980-9999 **Note** * Port 65101 is open and listening to support the access proxy process. The RealPresence Access Director system automatically redirects connections on port 389 to port 65101 to enable access proxy to function without root ownership of the process within the CentOS operating system.
Internal IP address	The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards LDAP requests from this IP address to the requested application server.
Next hop address	The internal IP address of the target LDAP server. After accepting a communication request from an endpoint client, the RealPresence Access Director system sends a new request to the next hop IP address on behalf of the external client.
Next hop port	The port at which the internal LDAP application server listens. Default LDAP port: 389
Require client certificate from the remote endpoint	When selected, access proxy requests and verifies the client certificate from the remote endpoint.
Verify certificate from internal server	When selected, access proxy verifies the certificate from the internal LDAP server.

5 Click **Done**, then click **OK** to confirm the configuration settings and restart access proxy.

Configuring XMPP Proxy Settings

XMPP reverse proxy configurations can be added to access different XMPP servers, such as the XMPP server configured in the RealPresence Resource Manager system or a different network server that provides message, presence or other XMPP services.

To configure XMPP proxy settings

1 Go to **Configuration > Access Proxy Settings**.

2 Under **Actions**, click **Add**.

3 In the **Step 1 of 2: Protocol Selection** window, select **XMPP** from the **Protocol** list and click **Next**.

4 In the **Step 2 of 2: Detailed Settings** window, complete the fields according to the table below:

Setting	Description
Name	The unique name of this XMPP proxy configuration
External IP address	The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.
External listening port	The external port at which the RealPresence Access Director system listens for XMPP traffic. Default **XMPP_proxy** port: 5222 Port range: 9980-9999
Internal IP address	The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards XMPP requests from this IP address to the requested application server.
Next hop address	The internal IP address of the target XMPP server. After accepting a communication request from an endpoint client, the RealPresence Access Director system sends a new request to the next hop IP address on behalf of the external client.
Next hop port	The port at which the internal XMPP application server listens. Default XMPP port: 5222
Require client certificate from the remote endpoint	When selected, access proxy requests and verifies the client certificate from the remote endpoint. **Note** Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence Access Director system. Remote clients must also install a client certificate and trusted CA certificates.
Verify certificate from internal server	When selected, access proxy verifies the certificate from the internal LDAP server. **Note** Before enabling this setting, an administrator must install a Server SSL certificate and trusted CA certificates on the RealPresence Access Director system and the RealPresence Resource Manager system.

5 Click **Done**, then click **OK** to confirm the configuration settings and restart access proxy.

Understanding Passthrough Proxy

A passthrough reverse proxy configuration provides transparent relay of communication requests through the RealPresence Access Director system to internal application servers. Passthrough reverse proxy is used primarily for backwards compatibility with the TCP reverse proxy feature and appears on the main

Access Proxy Settings page after upgrading the system software only if you configured a TCP reverse proxy in the previous version of the RealPresence Access Director system.

Reverse proxy connections to a RealPresence CloudAXIS Suite Experience Portal or Services Portal server should be configured as next hops based on the Host header filter within the default **HTTPS_proxy**, or a new HTTPS reverse proxy configuration. See To configure HTTPS proxy settings on page 57.

For security purposes, Polycom does not recommend use of a passthrough reverse proxy.

Configuring HTTP Tunnel Settings

An HTTP tunnel reverse proxy provides firewall traversal for RealPresence CloudAXIS Suite clients making SIP guest calls to video conferences. Specifically, the HTTP tunnel reverse proxy allows external CloudAXIS Suite clients to accept meeting requests from internal enterprise users and join the meetings as SIP guest users via standard HTTP ports or non-standard ports that you configure as HTTP tunnel settings. An HTTP tunnel reverse proxy enables the RealPresence Access Director system to act as a Web proxy and provide a bidirectional SIP signaling and media relay connection for HTTP requests.

You must have at least two available external IP addresses for access proxy if both the HTTP tunnel reverse proxy and any HTTPS reverse proxy bind on port 443. If only one external IP address is available, the HTTP tunnel reverse proxy port must be different than the HTTPS reverse proxy port. For example, if HTTPS reverse proxy uses port 443, the HTTP tunnel reverse proxy could use port 80.

If you have configured only one network interface on your system, all WAN-based traffic is routed through the same external IP address and the access proxy function listens on port 443 for HTTP/HTTPS connection requests. In this case, you must specify a different external listening port, such as 80, for HTTP tunnel calls. Note that the network from which the CloudAXIS guest client calls may block calls going out to specific ports. If the external listening port you configure in HTTP tunnel settings is blocked by an external network, CloudAXIS guest client calls from that network to the blocked external listening port will fail.

Polycom recommends that you configure a separate network interface as the external IP address and assign port 443 as the external listening port for HTTP tunnel calls from CloudAXIS guest clients to a CloudAXIS Suite Services Portal or Experience Portal.

If a CloudAXIS guest client cannot use port 443 to join a meeting, please contact Polycom Global Services for support.at support.polycom.com.

The following conditions apply to the HTTP tunnel proxy:

- Only one HTTP tunnel proxy can be configured.
- The HTTP tunnel proxy supports only SIP guest calls.
- The RealPresence Access Director system supports a maximum of 50 concurrent HTTP tunnel calls. After a call ends, the system recycles the port allocation.

- An HTTP tunnel proxy cannot be used with two RealPresence Access Director systems deployed in a tunnel configuration.
- Binary Floor Control Protocol (BFCP) is not supported.

To configure an HTTP tunnel reverse proxy for CloudAXIS Suite external guest clients, complete the steps in each of these sections:

1. Assign external access proxy IP addresses in network settings
   See Access Proxy Settings on page 28
2. Configure the HTTP reverse proxy tunnel
   See Configuring HTTPS Proxy Settings on page 56
3. Configure the CloudAXIS Suite Services Portal and Experience Portal as next hops in HTTPS proxy settings
   See To add a next hop based on the Host header filter on page 58

To configure HTTP tunnel reverse proxy settings

1. Go to **Configuration > Access Proxy Settings**.
2. Under **Actions**, click **Add**.
3. In the **Step 1 of 2: Protocol Selection** window, select **HTTP Tunnel** from the **Protocol** list and click **Next**.
4. In the **Step 2 of 2: Detailed Settings** window, complete the fields according to the table below:

Setting	Description
Name	The name of the HTTP tunnel reverse proxy configuration
External IP address	The external IP address of the network interface that receives HTTP tunnel reverse proxy traffic.
External listening port	The external port at which the RealPresence Access Director system listens for HTTP tunnel requests. HTTP tunnel port range: 80, 443, 9980-9999

5. Click **Done**, then click **OK** to confirm the configuration settings and restart access proxy.

Editing Proxy Configurations

To edit a proxy configuration

1. Go to **Configuration > Access Proxy Settings**.
2. Select the proxy to edit.
3. Under **Actions**, click **Edit**, then click **Next** to bypass the **Step 1 of 2: Protocol Selection** window.
4. In the **Step 2 of 2: Detailed Settings** window, revise the settings as needed.
5. Click **Done**.

6 Click **OK** to confirm the changes and restart access proxy.

Deleting Proxy Configurations

To delete a proxy configuration

1 Go to **Configuration > Access Proxy Settings**.

2 Select the proxy to delete.

3 Under **Actions**, click **Delete**.

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

Configuring SIP Signaling Settings

The RealPresence Access Director system operates as a SIP Back-to-Back User Agent (B2BUA), enabling SIP videoconferencing sessions between remote endpoints and internal enterprise network endpoints. Specifically, the SIP B2BUA enables the following:

- Firewall traversal for SIP signaling from remote clients to the internal SIP proxy server (the RealPresence DMA system)
- Sending of outgoing SIP signaling messages to remote and SIP open (unfederaed) B2B clients
- Federated connections with other organizations

After initial installation, the RealPresence Access Director system has two pre-configured external ports. The table below lists the settings for each port.

Port Name	Port Number	Transport Type	Certificate	Dial String Policy
Unencrypted	5060	UDP/TCP	Not required	
Encrypted	5061	TLS	Not required	Disabled

The system also has default internal SIP port settings to support the access configuration on the external ports. The internal ports communicate with the RealPresence DMA system, which acts as the SIP server and sends SIP signaling messages to the RealPresence Access Director system. The table below lists the internal port settings.

Port Name	Default Port Number	Transport Type
Unencrypted	5070 5070	UDP/TCP TCP
TLS port (encrypted)	5071	TLS

Configuring SIP Settings

To configure SIP settings

1. Go to **Configuration > SIP Settings**.
2. Select **Enable SIP signaling**.
3. Use the information in the table below to configure the settings for your system. An asterisk (*) indicates a required field.

Field	Description
External Port Settings	
* Port number	The external listening port the RealPresence Access Director system uses to receive SIP signaling messages to be forwarded to a RealPresence DMA system gatekeeper. **Note** Polycom recommends that you use the default port number 5060 for UDP/TCP and 5061 for TLS, but you can use any value from 5060-5100 or 65400-65499 that is not already in use.
* Port name	The descriptive name for the port.
Transport	The transport protocol of the port.
Require certificate from remote endpoint	Specifies whether the external port requires a certificate from the remote endpoint.
Default contact port for SIP open B2B	The listening port the RealPresence Access Director system uses to receive SIP request messages from SIP endpoints that are not registered or are not members of a federated enterprise or division. The RealPresence Access Director system routes SIP open B2B calls only if you specify a valid default contact port for each type of transport. The default SIP ports are: TCP, UDP: 5060 TLS over TCP: 5061 You can designate other unused ports as the default contact ports if preferred. Only one default contact port can be configured for each type of transport.
Dial string policy	When enabled, the RealPresence Access Director system uses a dial string prefix to route incoming SIP messages from the external port to a RealPresence DMA system.

Field	Description
Prefix of Userinfo	The dial string prefix that the RealPresence Access Director system adds to the request line of the SIP INVITE message that is routed to the RealPresence DMA system. **Note** This dial string prefix must also be defined in the RealPresence DMA system.
Host	Specifies the host IP address or FQDN to use in the dial string if you want to change the default dial string host. **Caution** If you define a new host, the host must also be defined in the RealPresence DMA system. If not defined, the DMA system will reject calls from the new host.
Internal Port Settings	
* Unencrypted port	The transport protocol the RealPresence Access Director system uses for unencrypted SIP calls and the internal listening port the system uses for SIP signaling messages from the RealPresence DMA system gatekeeper. Default UDP/TCP port: 5070 **Note** Polycom recommends that you use the default port numbers, but you can use any value from 5060-5100 or 65400-65499 that is not already in use and is different from the TLS port.
* TLS port	The internal listening port the RealPresence Access Director system uses for TLS-encrypted SIP signaling messages from the RealPresence DMA system gatekeeper. Default TLS port: 5071 **Note** Polycom recommends that you use the default port number, but you can use any value from 5060-5100 or 65400-65499 that is not already in use and is different from the UDP/TCP port. If SIP signaling is enabled, TLS is automatically supported.

Field	Description
* SIP registrar (Next hop) address, Port, and Transport	The IP address or FQDN of the SIP registrar server, and the destination port number and transport protocol the system uses to communicate with the SIP registrar server. The port number of the SIP registrar server must be the same as the port on which the SIP server in the RealPresence DMA system listens. The transport protocol must be supported by the SIP registrar server. Default TCP and UDP port: 5060 Default TLS port: 5061 Default transport protocol: TCP **Note** Polycom recommends that you use the default port number 5060 for UDP and TCP, and port number 5061 for TLS; however, you can use any value from 5060-5100 or 65400-65499 that is not already in use. When AUTO is selected, the transport protocol depends on the DNS query result for the SIP registrar address. Only TCP and TLS are available for transport when TCP is selected for the unencrypted SIP port.
* SIP proxy (Next hop) address, Port, and Transport	The IP address or FQDN of the internal SIP proxy server to which the RealPresence Access Director system forwards SIP registration or SIP call routing communication from endpoints. The RealPresence DMA system acts as the SIP proxy server so this is the DMA system IP address. The port number of the SIP proxy server must be the same as the port on which the SIP server in the RealPresence DMA system listens. The transport protocol must be supported by the SIP proxy server. Default TCP and UDP port: 5060 Default TLS port: 5061 Default transport protocol: TCP **Note** Polycom recommends that you use the default port number (5060) for UDP and TCP, and port number 5061 for TLS; however, you can use any value from 65400-65499 that is not already in use. When AUTO is selected for transport, the transport protocol depends on the DNS query result for the SIP proxy address. Only TCP and TLS are available for transport when TCP is selected in the **Unencrypted port** field.

Field	Description
* Registration refresh interval	Specifies how often registered SIP endpoints send keep-alive messages to the SIP registrar server to refresh the existing call registration. Endpoints that fail to send keep-alive messages on time must send a new registration request. Must be greater than or equal to the minimum SIP registration interval that the SIP registrar server allows. Default: 300 seconds Range: 1–99999 seconds
* RFC5626 keep-alive interval	The `Flow-Timer` value used by the SIP registrar to specify after how many seconds the registrar will consider the call dead if no keep-alive message is sent by an RFC5626 endpoint. Default: 120 seconds Range: 1-99999 seconds

4 Click **Update** to save the settings.

The SIP service restarts.

Adding an External SIP Port

To add an external port

1 Go to **Configuration > SIP Settings**.

2 Select **Enable SIP signaling**.

3 Click **Add** next to the **External Port Settings** list.

4 Complete the external port settings as described in the table in Configuring SIP Settings on page 65.

5 Click **OK**.

6 Click **Update**.

Editing an External SIP Port

To edit an external SIP port

1 Go to **Configuration > SIP Settings**.

2 Select the port to edit in the **External Port Settings** table.

3 Click **Edit**.

4 Modify the port information as needed.

5 Click **OK.**

6 Click **Update**.

Deleting an External SIP Port

To delete an external SIP port

1. Go to **Configuration > SIP Settings**.
2. Select the port to delete in the **External Port Settings** table.
3. Click **Delete** and **Update**.
4. Click **Yes** to confirm the deletion.

Configuring H.323 Signaling Settings

The RealPresence Access Director system supports the H.323 protocol for call signaling and control for videoconferencing sessions.

When a remote H.323 client sends a registration request to the RealPresence Access Director system, the system proxies the registration request to the enterprise gatekeeper (the RealPresence DMA system) to enable the H.323 call.

The RealPresence Access Director system also supports remote H.323 users with H.460-enabled endpoints. The H.460.18 (signaling) and H.460.19 (media) standards enable traversal of H.323 signaling across firewalls and network address translators (NATs). To support H.460, the RealPresence Access Director system does the following:

- Uses the H.460.18 registration procedure to proxy registration requests from H.460-enabled endpoints to the gatekeeper.
- Enables the keep-alive mechanism of H.460.19 for opening and maintaining Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) pinholes in the firewall for communication between the remote endpoint and the gatekeeper.

The RealPresence Access Director system supports symmetric media communication. This means that remote H.460 endpoints must use the same port to send and receive one media stream.

To configure H.323 settings

1. Go to **Configuration > H.323 Settings**.
2. Use the information in the table below to configure the settings for your system.

   An asterisk (*) indicates a required field.

Field	Description
Enable H.323 signaling	Enables the system to operate as an H.323 server, transmitting H.323 requests and responses for H.323 endpoints. **Caution** Disabling H.323 terminates any existing H.323 calls.
Internal port settings	
* H.225 RAS port	The internal listening port the RealPresence Access Director system uses for receiving Registration, Admission, and Status (RAS) messages from the RealPresence DMA system gatekeeper. Default: 1719 Polycom recommends that you use the default port number, but you can use any value from 1700-1800 or 65400-65499 that is not already in use.
* H.225 call signaling port	The internal listening port the RealPresence Access Director system uses for receiving Q.931 signaling messages from the RealPresence DMA system gatekeeper. Default: 1720 **Note** Polycom recommends that you use the default port number, but you can use any value from 1700-1800 or 65400-65499 that is not already in use.
External port settings	
* H.225 RAS port	The external listening port the RealPresence Access Director system uses for receiving Location Request (LRQ) messages to be forwarded to the RealPresence DMA system gatekeeper. Default: 1719 **Note** Polycom recommends that you use the default port number, but you can use any value from 1700-1800 or 65400-65499 that is not already in use.
* H.225 call signaling port	The external listening port the system uses for receiving Q.931 signaling messages to be forwarded to the RealPresence DMA system gatekeeper. Default: 1720 **Note** Polycom recommends that you use the default port number, but you can use any value from 1700-1800 or 65400-65499 that is not already in use.
* Gatekeeper (Next hop) address	The IP address or FQDN of the H.323 gatekeeper.

Field	Description
* RAS port	The listening port of the RealPresence DMA system gatekeeper. The RealPresence Access Director system forwards LRQ messages to this port. **Note** Polycom recommends that you use the default port range 0-65535.
* H.225 call signaling port	The listening port of the RealPresence DMA system gatekeeper. The RealPresence Access Director system forwards Q.931 signaling messages to this port. **Note** Polycom recommends that you use the default port range 0-65535
CIDR	In the RealPresence Access Director system, CIDR notations include the IP address and subnet of local network H.323 devices (e.g., the DMA system gatekeeper, endpoints, and bridges). You should add CIDR notations that specify all of the IP spaces within your enterprise LAN that include H.323 devices.
Enable H.323 guest policy	When enabled, the RealPresence Access Director system adds a prefix to the dial string when forwarding H.323 guest calls from an external network to the RealPresence DMA system. Default: disabled
Prefix to dial string	If H.323 guest policy is enabled, the RealPresence Access Director system adds the prefix you specify to the dial string when forwarding H.323 guest calls from an external network to the RealPresence DMA system.
Enable H.323 default policy	Select to enable the RealPresence Access Director system to assign a default destination alias to incoming H.323 guest calls that do not already include a destination alias in the Q.931 call SETUP message. The RealPresence Access Director system uses the default destination alias you specify to route H.323 guest calls to the RealPresence DMA system. The system uses two types of default aliases to associate a call from an H.323 guest endpoint with a specific gatekeeper: • E.164 • H.323_ID
E.164	A default destination alias string that consists of numbers, e.g., a meeting room number or extension number.
H.323_ID	A default destination alias string that consists of alphanumeric characters, e.g., a meeting room name or customer's name.

Field	Description
H.460 settings	
External registration refresh interval	Specifies how often registered endpoints send keep-alive messages to the RealPresence Access Director system to refresh the existing call registration. Endpoints that fail to send keep-alive messages on time must send a new registration request. Default value: 60 seconds Range: 15–150 seconds
Internal registration refresh interval	Specifies how often the RealPresence Access Director system sends keep-alive messages to the RealPresence DMA system to refresh the existing call registration. Default: 300 seconds Range: 150–9999 seconds

If both **Enable H.323 guest policy** and **Enable H.323 default policy** are enabled, the RealPresence Access Director system uses the default destination alias you specify to forward H.323 guest calls to the RealPresence DMA system.

3 Click **Update** to save the settings.

To add a CIDR address

1 Go to **Configuration > H.323 Settings**.

2 In the **CIDR** fields, enter the IP address and the routing prefix size of the local network subnet that includes H.323 devices.

3 Click **Add**.

The CIDR address displays in the CIDR list.

4 Enter a separate CIDR address for each subnet that has H.323 devices.

To delete a CIDR address

1 Go to **Configuration > H.323 Settings**.

2 In the CIDR address list, select the IP address to delete and click **Delete**.

Configuring Media Traversal Settings

The media relay component of the RealPresence Access Director system enables media connections to traverse the firewall during SIP and H.323 calls.

To configure the media traversal settings

1. Go to **Configuration > Media Traversal Settings**.
2. Configure the settings as described in the following table.

Field	Description
Media Relay	
External Relay IP Address	The external IP address of the RealPresence Access Director system network interface that receives media relay requests from remote users.
Internal Relay IP Address	The internal IP address of the RealPresence Access Director system network interface used to forward media relay requests to the RealPresence DMA system and receive media relay responses from the DMA system.
Band Width Limitation	Specifies the total available media bandwidth. When the total bandwidth is used by all active calls, the next call request will be rejected The default value is 256 Mbps.
Enable QoS	When enabled, allows you to select the Quality of Service (QoS) for the media packets relayed by the system.
QoS Setting	Specifies 20 classes of differentiated services (DiffServ) that enable you to set the priority of media packets relayed by the system for video, audio, and far-end camera control. The default setting is disabled. **Note** Polycom recommends that you use the default value **Real-Time Interactive** when QOS is enabled. For detailed implications for each Diffserv type, refer to RFC4594.

3. Under **Actions**, click **Update** to save the settings.

For more information on configuring media traversal settings, refer to the *Polycom RealPresence Access Director Deployment Guide*.

Configuring Federation Settings

The RealPresence Access Director system enables enterprise users from one division or enterprise to call enterprise users from other federated, or neighbored, divisions or enterprises.

Federated divisions or enterprises have established a trust connection. For SIP systems, this trust relationship is a SIP trunk between two or more RealPresence Access Director systems, or between a RealPresence Access Director system and a different session border controller. For H.323 systems, this trust relationship is mutually neighbored gatekeepers.

For additional information about federations, see *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*.

Viewing Current Enterprise Federations

1 Go to **Configuration > Federation Settings**.

The system displays details about currently federated companies or divisions.

Field	Description
Name	The name of the company name with which you have a federated connection.
Company Address	The domain name or IP address of the federated company.
First Remote Listen Port	SIP: remote listen port H.323: H.225 RAS port
Second Remote Listen Port	SIP: Not applicable. H.323: Remote H.225 signaling port.
Local Contact Port	The local contact port for the SIP trunk or H.323 gatekeeper.
Type	The type of federated connection (**SIP** or **H.323**).
Status	The status of the connection (**Active** or **Inactive**).

Searching for a Federation

1 Go to **Configuration > Federation Settings**.

2 Complete the **Type**, **Status**, and **Company Name** fields as needed and click **Search**.

Adding a New Federation

To create a new federation

1 Go to **Configuration > Federation Settings**.

2 Under **Actions**, click **Add**.

3 In the **Add Company** window, complete the following fields for the new trust connection:

Field	Description
Company Name	The name of the company with which you are creating a new federation.
Type	The type of federated connection (**SIP** or **H.323**).
Company Address	The domain name or IP address of the federated company.
Remote Listen Port	The listening port of the trusted SIP peer.
Remote H.225 RAS Port	RAS port of the trusted neighbor gatekeeper or H.323 proxy. Applicable for H.323 only

Field	Description
Remote H.225 Signaling Port	The H.225 call signaling port of the trusted neighbor gatekeeper or H.323 proxy. Applicable for H.323 only.
Local Contact Port	The local contact port for the SIP trunk or H.323 gatekeeper.
Status	The status of the connection (**Active** or **Inactive**).

4 Click **OK**.

Editing a Federation

To create a new federation

1 Go to **Configuration > Federation Settings**.

2 Under **Actions**, click **Edit**.

3 In the **Edit Company** window, revise the federation settings as needed.

4 Click **OK** to save the new settings.

System Administration and Additional Configuration

After configuring the key settings for the Polycom® RealPresence® Access Director™ system (see System Configuration on page 19), you can customize additional system settings based on your firewall and network requirements. See these topics for detailed instructions:

Setting Custom Security for Network Access

The custom security settings specify options for controlling network access, as described below:

- **Allow Linux SSH access**: When enabled, allows remote Secure Shell access to the RealPresence Access Director system console.
- **Enable access proxy white list authentication for LDAP and XMPP access**: When enabled, the RealPresence Access Director system denies all LDAP and XMPP requests from endpoints that are not on the system's white list.
- **Enforce TLS for LDAP connection**: When enabled, the RealPresence Access Director system denies all LDAP connection requests from remote endpoints that are sent without TLS encryption.

Only administrators can enable and disable custom security settings.

To enable or disable network access methods

1. Go to **Admin > Security Settings**.
2. Select or deselect the custom security options.

3 Click **Update**.

4 Click **Yes** to confirm your selections.

Using Access Control List Rules

Access Control List rules serve as filters for SIP and H.323 registration messages that come through the external signaling ports. The rules define whether the RealPresence Access Director system allows or denies a specific type of SIP or H.323 request from a public network.

The Access Control List features provide numerous options for defining access rules and are highly configurable. You can use Access Control List rules to create white lists, black lists, and other access controls. Additionally, multiple Access Control List rules can be applied on one port.

Defining and applying an Access Control List rule involves three steps:

- Define an Access Control List rule and its conditions. See on page 81.
- Specify variables to apply to the Access Control List rules (optional). See Using Access Control List Variables on page 85.

  If you plan to use custom variables for a rule condition, you should define the variables first, before you create or edit the rule and its conditions.
- Apply the Access Control List rule and the associated action (rule setting) to a specific external port. See Configuring Access Control List Settings on page 86.

The **Access Control List Rules** page displays all Access Control List rules, including the RealPresence Access Director system default rules (see Using the Default Access Control List Rules on page 78). When you select a rule from the rules list, general information displays about that rule.

The table below describes the information on the **Access Control List Rules** page.

Field	Description
Rule Name	The name of the rule. **Note** A rule name cannot contain blank spaces.
Service	The type of service to which the rule applies. **SIP**, **H.323**, or **Common** (both services)
General Info	
Name	When you select a **Rule Name**, the name of the rule displays under **General Info**.
Description	The description of the rule you selected.

Field	Description
Condition	Lists the conditions for the rule you selected. A condition includes an attribute, operator, and value. If a rule has more than one condition, a relation defines how the conditions are applied relative to each other. **and**: If a message meets all of the conditions in the rule, the action for the rule is applied to the message. **or**: If a message meets any one of the conditions in the rule, the action for the rule is applied to the message. **And** and **or** display as folders, Click the folder to display all conditions for the relation.
Attribute	When you select a condition, lists the attribute or attributes for the condition. Attributes specify the fields in a SIP or H.323 request message.
Operator	When you select a condition, lists the operator for the condition. An operator compares the Attribute and Value fields of the condition. For any attribute you choose, the operator you select determines the available values for the condition.
Value	When you select a condition, lists the values for the specific attribute and operator of that condition. A value is dependent on the attribute and operator.

Working with Access Control List Rules

The topics below describe the actions you can perform from the **Access Control List Rules** page.

- Using the Default Access Control List Rules on page 78
- Adding an Access Control List Rule and Conditions on page 82
- Copying an Access Control List Rule on page 82
- Editing or Deleting an Access Control List Rule on page 83
- Editing or Deleting a Condition for an Access Control List Rule on page 83

Using the Default Access Control List Rules

The RealPresence Access Director system contains a number of pre-configured rules. These default rules and their conditions can be used as-is or edited to fit your needs.

To use one of the default rules, you must create an Access Control List setting that defines where to apply the rule, on which signaling type(s), and the action to perform when the system applies the rule to incoming call and registration requests. For details, see Configuring Access Control List Settings on page 86.

The table below lists the default Access Control List rules included in the RealPresence Access Director system. Select a rule from the list of rules on the **Access Control List Rules** page to view its configuration and conditions.

Name of Rule	Description	Service
Access_Without_Resource Manager_Provision	The RealPresence Access Director system records all IP addresses of remote endpoints and adds them to a provisioning list if the endpoint is authenticated during the VC2 provisioning process. When this rule is applied on a port, all incoming requests from IP addresses that are not on the provisioning list are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to deny access for SIP and H.323 services to endpoints not on the provisioning list. For instance, apply this rule on SIP port 5060 and assign **deny** as the rule setting action. **Note** If two endpoints are behind the same Firewall/NAT, both may share one public IP address. If one endpoint is provisioned and the other is not, this rule is not applied and both endpoints are able to access port 5060.	Common
All_Matches	When this rule is applied to a port, all incoming requests on that port are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to change the default access policy. For example, a port is accessible by default without any access policy. To change the default behavior so that access is denied, apply this rule to the port and assign **deny** as the rule setting action.	Common
H323_Guest_Call	When this rule is applied to an H.323 call signaling port, all incoming H.323 call requests on the port from non-registered H.323 guest endpoints are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to reject guest H.323 calls from the Internet to an H.323 signaling port. For example, apply this rule on H.323 port 1720 and assign **deny** as the rule setting action.	H.323

Name of Rule	Description	Service
H323_Guest_Call_Not_To_71xxxx_bridge	When this rule is applied to an H.323 call signaling port, all incoming H.323 guest call requests on that port that match the dial string in the rule are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to allow guest H.323 calls from the Internet to access *only* the 71xxx bridge. For example, apply this rule on H.323 port 1720 and assign **deny** as the rule setting action.	H.323
H323_Register_Call	When this rule is applied to an H.323 RAS port, all incoming H.323 call requests on the port from registered H.323 endpoints are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to allow incoming H.323 call requests from registered H.323 endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign **accept** as the rule setting action.	H.323
H323_Registration	When this rule is applied to an H.323 RAS port, all incoming H.323 registration requests on the port from H.323 endpoints are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to allow incoming H.323 registration requests from H.323 endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign **accept** as the rule setting action.	H.323
H323_Registration_Without_Polycom _Endpoint	When this rule is applied to an H.323 RAS port, all incoming H.323 registration requests on the port from non-Polycom H.323 endpoints are accepted or denied, depending on the rule setting you apply. This rule has conditions that distinguish a Polycom endpoint's product ID from other vendors in the RRQ. **Example** Use this rule to allow incoming H.323 registration requests from non-Polycom endpoints. The conditions for the rule specify that the vendor IDs do not match Polycom RealPresence Desktop, RealPresence Group, RealPresence Mobile, and HDX endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign **accept** as the rule setting action.	H.323

Name of Rule	Description	Service
SIP_Friendly_Scanner	When this rule is applied to a SIP port, all incoming SIP requests on that port that contain the user-agent header value `friendly-scanner` are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to deny incoming SIP requests that contain the user-agent header value `friendly-scanner`. For example, apply this rule on SIP port 5061 and assign **deny** as the rule setting action.	SIP
SIP_Guest_Call	When this rule is applied to a SIP call signaling port, all incoming SIP call requests on the port from non-registered SIP guest endpoints are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to reject SIP guest calls from the Internet to a SIP signaling port. For example, apply this rule on SIP port 5061 and assign **deny** as the rule setting action.	SIP
SIP_Guest_Call_Not_To_71xxxx_bridge	When this rule is applied to a SIP call signaling port, all incoming SIP guest call requests on that port that match the dial string in the rule are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to allow guest SIP calls from the Internet to access *only* the 71xxx bridge. For example, apply this rule on SIP port 5061 and assign **deny** as the rule setting action.	SIP
SIP_Registration	When this rule is applied to a SIP port, all incoming SIP registration requests on the port are accepted or denied, depending on the rule setting you apply. **Example** Use this rule to allow incoming SIP registration requests. For instance, apply this rule on SIP port 5060 and assign **accept** as the rule setting action.	SIP

Adding an Access Control List Rule and Conditions

To add a new Access Control List rule and conditions

1. Go to **Configuration > Access Control List Rules** and click **Add**.
2. Enter a name for the rule, such as *SIP_Call_Blacklist*.

   Do not use blank spaces in the name.
3. Select the type of service and enter a description of the rule.

   For the example rule name above, select **SIP** as the service type.
4. Click **Add** to add a condition for the rule and select the **Attribute**, **Operator**, and **Value** for the condition. The table below illustrates an example of a condition for the rule SIP_Call_SIP_Reg_List.

Condition	Description	Example String
Attribute	Select the type of request for which the rule applies	**request.from**
Operator	Select the operator that indicates what the value must be in relation to the attribute.	**memberOf**
Value	Select from the list of predefined values for specific attributes, or select a custom variable. See Adding a Variable on page 86.	**var_Blacklist** (custom variable)

5. Click **OK** to add the condition to the rule.
6. Add other conditions to the rule as needed.

You can define multiple conditions for each rule you create. When you define the first condition, the **Relation** field is not active. When you add subsequent conditions, select the relation for each condition.

7. Click **OK** to return to the **Access Control List Rule**s page.
8. Configure the Access Control List settings as described in Adding an Access Control List Setting on page 86.

Copying an Access Control List Rule

If you need to create a new Access Control List rule that is similar to an existing rule, you can copy the existing rules and revise it as needed.

To copy an Access Control List rule

1. Go to **Configuration > Access Control List Rules** and select the Access Control List rule to copy from the **Rule Name** list.
2. Under **Actions**, click **Copy**.

3 Enter a new name for the rule and revise, add, or delete the conditions as needed.

4 Click **OK** to create the new rule.

Editing or Deleting an Access Control List Rule

Access Control List rules can be edited at any time to revise general or condition information. Rules can also be deleted, but only if they are not used in any Access Control List settings. See Adding an Access Control List Setting on page 86.

To edit an Access Control List rule

1 Go to **Configuration > Access Control List Rules** and select the Access Control List rule to edit from the **Rule Name list**.

2 Under **Actions**, click **Edit**.

3 Revise the **General Info** as needed.

4 Click **OK** to save the changes to the Access Control List rule.

To edit conditions for an Access Control List rule, see Editing or Deleting a Condition for an Access Control List Rule on page 83.

To delete an Access Control List rule

1 Go to **Configuration > Access Control List Rules** and select the Access Control List rule to delete from the **Rule Name list**.

2 Under **Actions**, click **Delete > Yes**.

The rule is deleted from the rule list.

Editing or Deleting a Condition for an Access Control List Rule

To edit a condition for an Access Control List rule

1 Go to **Configuration > Access Control List Rules** and select the Access Control List rule that has the condition you want to edit.

2 Under **Actions**, click **Edit**.

3 Select the condition to revise and click **Edit**.

4 Select new definitions for the condition as needed.

5 Click **OK** to save the revised condition information.

6 Select and edit other conditions if necessary.

7 Click **OK** to save the changes to the Access Control List rule.

To delete a condition for an Access Control List rule

1. Go to **Configuration > Access Control List Rules** and select the Access Control List rule with the condition(s) to delete.
2. Under **Actions**, click **Edit**.
3. Select the condition to delete and click **Delete**.

   The condition is removed from the Access Control List rule.
4. Click **OK** to save the changes to the Access Control List rule.

Example: Defining an Access Control List Rule to Deny SIP Registration

To create an Access Control List rule to deny SIP registration on an external port

1. Go to **Configuration > Access Control List Rules** and click **Add** to create a new rule.
2. Enter a name for the rule, such as ACL-Deny-SIP-REGISTER.

   Do not use blank spaces in the name.
3. Select **SIP** and enter a description of the rule.
4. Click **Add** and select the following options:
   - **Attribute: request.method**
   - **Operator: = =**
   - **Value: REGISTER**
5. Click **OK** twice.
6. Go to **Configuration > Access Control List Settings**.
7. Click **Add** and select the following options:
   - **Service Name: SIP**
   - **IP**: The IP address of the network interface assigned to external signaling.
   - **Port**: The external SIP port on which the system will deny SIP registrations.
8. Click **Add** and select the following options:
   - **Access Control List Name**: the rule you created to forbid SIP registration (e.g., ACL-Deny-SIP-REGISTER)
   - **Action: Deny**
9. Click **OK**.

   The setting displays in the **Rule Setting** list.
10. Click **OK** to apply the rule.

Using Access Control List Variables

Variables, while optional, provide an efficient way to define group members, source IP addresses, and other lists. You can create custom variables and add values (list items) to the variables. A variable, with all of its component values, can then be applied to a condition for Access Control List rules, depending on the attribute and operator you select for the condition.

If you plan to create rules with one or more conditions that contain custom variables, you may want to create the variables first so they appear in the value field when you add a condition that uses a custom variable.

The RealPresence Access Director system maintains three system variables. You may select each variable as the value for certain rule condition attributes, as described in the following table:

Variable	Description	Associated Attribute
prov_list	All endpoints that are successfully provisioned by the RealPresence Resource Manager system through the RealPresence Access Director system.	`src.ip`
h323_reg_list	All H.323 endpoints that successfully register through the RealPresence Access Director system.	`src.address`
sip_reg_list	All SIP endpoints that successfully register through the RealPresence Access Director system.	`src.address`

These variables cannot be edited and are automatically updated by the RealPresence Access Director system.

Adding a Variable

To add an Access Control List variable

1. Go to **Configuration > Access Control List Variables** and click **Add**.
2. Complete the following fields:
   - **Name**: Enter a name for the variable, such as Whitelist or Blacklist.
   - **Value**: Enter a value to include in this variable, such as an IP address.
3. Click **Add** to add the value to values list.
4. Add additional values as needed.
5. Click **OK**.

Editing or Deleting a Variable

To edit an Access Control List variable

1. Go to **Configuration > Access Control List Variables** and select the variable to edit.
2. Under **Actions**, click **Edit**.
3. Add or delete values for the variable as needed.
4. Click **OK**.

To delete an Access Control List variable

1. Go to **Configuration > Access Control List Variables** and select the variable to delete.
2. Under **Actions**, click **Delete > Yes**.

   The variable is deleted from the list of variables.

Configuring Access Control List Settings

An Access Control List setting allows you to apply one or more rule settings to the same signaling type, IP address, and port.

A rule setting combines an Access Control List rule with the action the RealPresence Access Director system performs when it applies the rule to incoming calls. The system applies rule settings according to the order of priority you define.

Adding an Access Control List Setting

From the **Access Control List Settings** page, you can view current Access Control List settings, create new settings, and edit or delete settings.

When you add, edit, or delete an Access Control List setting, all changes are effective immediately for new call requests. Active calls are not affected.

To add an Access Control List setting and rule setting

1. Go to **Configuration > Access Control List Settings** and complete the following fields:
   - **Service Name**: Select **SIP** or **H.323**.
   - **IP**: Select the external signaling IP address.
   - **Port**: Select the external port to which the Access Control List rule applies.
2. Click **Add** and complete the information below:
   - **Access Control List Name**: Select the Access Control List rule to use for this Access Control List setting.
   - **Action**: Select **Accept** or **Deny**.
3. Click **OK**.

   The setting displays in the **Rule Setting** list.
4. Repeat the previous steps to add additional rule settings.
5. Click **OK** to create the Access Control List setting.

To prioritize rule settings

You must have more than one Access Control List rule setting to assign a priority order for the settings.

1. Go to **Configuration > Access Control List Settings** and select an Access Control List to prioritize its rule settings.
2. Under **Actions**, click **Edit**.
3. Select a rule setting and click **Priority Up** or **Priority Down** to increase or decrease the priority of the rule setting. Repeat until the rule settings are listed (prioritized) in the order you want.
4. Click **OK** to apply the order of priority for the rule settings.

Editing or Deleting an Access Control List Setting

To edit an Access Control List setting

1. Go to **Configuration > Access Control List Settings** and select the Access Control List setting to edit.
2. Under **Actions**, click **Edit**.
3. Revise the following fields as needed:
   - **Service Name**: Select **SIP** or **H.323**.
   - **IP**: Select the external signaling IP address.

- **Port**: Select the external port to which the Access Control List rule applies.

4 Click **OK** to save the new settings or edit the rule settings if needed, as described in Editing or Deleting a Rule Setting on page 88.

To delete an Access Control List setting

1 Go to **Configuration > Access Control List Settings** and select the Access Control List setting to delete.

2 Under **Actions**, click **Delete > Yes**.

The setting is deleted from the list of Access Control List Settings.

Editing or Deleting a Rule Setting

To edit a rule setting

1 Go to **Configuration > Access Control List Settings** and select the Access Control List setting that contains the rule setting you want to edit.

2 Under **Actions**, click **Edit**.

3 Select the **Rule Setting** to revise and click **Edit**.

4 Revise the information below as needed:

- **Access Control List Name**: Select the Access Control List rule to use for this Access Control List setting.
- **Action**: Select **Accept** or **Deny**.

5 Click **OK** to apply the revised rule settings.

6 Click **OK** again to update the Access Control List setting.

To delete a rule setting

1 Go to **Configuration > Access Control List Settings** and select the Access Control List setting that contains the rule and action you want to delete.

2 Under **Actions**, click **Edit**.

3 Select the **Rule Setting** to delete and click **Delete**.

4 Click **OK**.

Configuring Log Settings

Log file settings can be configured to meet the specific parameters for your RealPresence Access Director system.

Only administrators can change log settings.

The table below describes the log file settings and their default values.

Field	Description	Default Value
Log file rolling		
Rolling frequency	The frequency at which the system rolls active log files into archive files. If rolling the logs daily (default setting) produces logs that are too large to manage, or if rolling log files are being overwritten, select a shorter interval.	Every day
Retention period (days)	The number of days that the system retains archived log files before deleting them. Range: 1 – 30 days Polycom recommends downloading archived log files before the end of the retention period.	7 days
Application log settings		
Logging level	The event severity level at which the system will start creating logs. For example, if the logging level is Error, the system will create only Error-level and Fatal-level logs.	Info
Log file size	The combined maximum size of the log file and packet captures. Range: 1 MB – 50 MB	50 MB
Remote syslog settings		
Transport	The transport protocol for sending log files to the remote server.	UDP
Remote IP	The IP address of the remote server where the log files will be stored. **Note** You can add a maximum of two remote log servers.	
Remote port	The listening port for syslog-ng on the remote server.	
Severity filter	The event severity filter to apply to the remote syslog server. If you have more than one remote server, you can specify different severity filters for each server.	Info

Configuring Log File Rolling and Application Log Settings

To set the rolling frequency, retention period, and logging level

1. Go to **Admin > Log Settings**.
2. Select the following settings for the system:
   - **Rolling frequency**: If rolling the logs daily (default setting) produces logs that are too large to manage, select a shorter interval.
   - **Retention period**: Number of days to keep archived log files.

     The default value is seven days. Consider the impact on disk space when specifying this period.
   - The **logging level** that you select generates messages as described in the following table:

Logging Level	Description
Debug	Detailed information used to debug the system. Using this level captures more information but consumes a higher level of system resources If you set the logging level to **Debug** to capture details for debugging, set the logging level back to the default **Info** when you finish debugging.
Info	Normal operational messages that highlight the progress of the system and do not require any action. **Info** is the default logging level.
Warn	Warning messages that indicate an error will occur if action is not taken.
Error	Non-urgent error events that must be resolved within a given time. These events may allow the system to continue running.
Fatal	Severe error events that will cause the system to abort.

   - The **Log file size** is the maximum size of each log file, ranging from 1 MB to 100 MB.

Configuring Remote Syslog Settings

To add a remote syslog server

1. Go to **Admin > Log Settings**.
2. In **Remote syslog settings**, click **Add**.
3. In **Remote setting**, complete the following fields:

Field	Description
Transport	The transport protocol the system uses to send log files to the remote server. Default value is UDP.
Remote address	The IP address of the remote server where the log files will be stored.
Remote port	The listening port for syslog-ng on the remote system.
Severity filter	The event severity filter to apply to the remote syslog server. Default value is Info. **Options** Debug Info Notice Warning Err Crit Alert Emerg

4 In **Source log files,** select the **Available source files** for syslog-ng to store as local log files and forward to the remote server:

- ACCESSPROXY
- ACTIVECALLAUDITOR
- DBACCESS
- H323SERVICE
- LICENSE
- SIPSERVICE
- SNMP
- WEBADMIN

5 Click  to add the source files to the **Selected source files** list.

6 Click **OK** to add the remote syslog server settings.

7 Click **Update** to process all changes to the log settings.

Working with SNMP Settings

Simple Network Management Protocol (SNMP) is a TCP/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.

The RealPresence Access Director system includes an SNMP agent. It translates local system information into the format defined by the Management Information Base (MIB). A MIB is the database commonly shared between an agent and the SNMP management system. In short, MIB files are the set of questions that the SNMP management system can ask the agent. The agent collects the data locally and makes this information available to the management system via SNMP.

SNMP traps allow the RealPresence Access Director system agent to notify the SNMP management system of significant events by sending out an unsolicited SNMP message. The data collected includes information about CPU, memory, storage, and the status of the system.

Note that you should understand how your SNMP management system is configured to accurately configure the SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements on the RealPresence Access Director system.

The RealPresence Access Director system supports three SNMP levels:

- **Disabled**—The RealPresence Access Director system SNMP processes are turned off.
- **SNMPv2c**—The RealPresence Access Director 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 Access Director system re-sends 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 Access Director system implements the newest version of SNMP. Its primary feature is enhanced security. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity and is used to generate the key for authenticated messages.

  The RealPresence Access Director system implements SNMPv3 communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB).

  To implement this security level, you must define SNMP users to be added to the SNMP agent user list. Agents use this list to protect SNMPv3 packets from interception. Each user has a secret key to ensure authentication and privacy.

  - Authentication ensures that 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.

Using SNMP Monitoring

To use SNMP monitoring, complete the steps below:

1. Go to **Admin > SNMP Settings** and select **Enable SNMP monitoring**.

   By default, SNMP monitoring is disabled after initial installation of a RealPresence Access Director system.
2. Configure the SNMP settings for the RealPresence Access Director system. See Configuring SNMP Settings on page 93.
3. Configure the Notification Users for the RealPresence Access Director system. See Configuring Notification Users on page 95.
4. Configure the Notification Agents for the RealPresence Access Director system. See Adding a Notification Agent on page 97.
5. Download the available MIBs as needed. See Downloading MIBs on page 98.

Configuring SNMP Settings

To configure SNMP settings

1. Go to **Admin > SNMP Settings**.
2. Select **Enable SNMP monitoring**.
3. Configure the settings in the table below for the connection between the RealPresence Access Director system and the notification agents you add. Depending on the SNMP version you select, different settings will display, as noted in the table.

Field	Description
Agent Setting	
SNMP version	Specifies the version of SNMP. When SNMP monitoring is enabled, the RealPresence Access Director system supports two SNMP versions: • v2c • v3
Transport	Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols: **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.

Field	Description
Port	Specifies the port that the RealPresence Access Director system uses for general SNMP messages. By default, the system uses port 161. Polycom recommends that you use the default port number 161, but you can use any value from 65390-65399 that is not already in use.
Community	Specifies the community name, which is the name of the SNMP group to which the devices and management stations running SNMP belong. The RealPresence Access Director system's SNMP agent is a member of only one community. The default name is `public`, but you should change the name for security reasons. The community name is essentially a password. The RealPresence Access Director system will not respond to requests from SNMP management systems that don't belong to the same community. By itself, this provides only a minimal level of security; since SNMPv2c doesn't encrypt communications, the community name is sent in clear text. SNMPv3 provides much greater security.
Local engine ID	For both SNMPv2c and SNMPv3, displays the RealPresence Access Director system `contextEngineID`.
Security user	For SNMPv3, specifies the security name required to access a monitored MIB object.
Authentication type	For SNMPv3, specifies the authentication protocol. These protocols are used to create unique, fixed-size message digests of a variable length message. The RealPresence Access Director 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.
Authentication password Confirm 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 Access Director system and the SNMP agent. The RealPresence Access Director system implements communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB).
Encryption password Confirm password	For SNMPv3, specifies the password to be associated with the privacy protocol.

4 Click **Update**.

5 To enable notifications (Traps or Informs) to specified users/hosts, do the following:

- If using SNMPv3, add one or more notification users (see Configuring Notification Users on page 95).
- Add one or more notification agents (see Adding a Notification Agent on page 97).

Configuring Notification Users

For SNMPv3 notifications, you must specify at least one security user who is authorized to receive notifications. You can add the first security user on the **Agent Setting** tab by completing the following fields. See the table in To add an SNMP notification user on page 95 for a descriptions of the fields.

- Security user
- Authentication type
- Authentication password
- Confirm password
- Encryption type
- Encryption password
- Confirm password

The **Add Notification User** dialog box on the **Notification Setting** tab lets you add additional security users to the RealPresence Access Director system. When you add a notification agent, you select a security user from the list of notification users.

Notification users aren't needed or used for SNMPv2c.

Adding a Notification User

To add an SNMP notification user

1 Go to **Admin > SNMP Settings > Notification Setting**.

2 In the **Notification Users** section, click **Add User**.

3 Configure the settings in the **Add Notification User** dialog box.

Field	Description
Notification Setting	
Notification Users (USM)	Lists the notification users that have been created. For SNMPv3, these are security users authorized to receive notifications (Traps or Informs), but not to actively retrieve SNMP data. Notification agents can send notifications to users in this list.
Security user	For SNMPv3, specifies the security name required to access a monitored MIB object.

Field	Description
Authentication 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 Access Director 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.
Authentication password Confirm 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 Access Director system and the SNMP agent. The RealPresence Access Director system supports three settings: • No encryption. • DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet. • AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet.
Encryption password Confirm password	For SNMPv3, specifies the password to be associated with the privacy protocol.

4 Click **OK**.

The user appears in the **Notification Users** list.

Editing a Notification User

To edit a notification user

1 Go to **Admin > SNMP Settings > Notification Setting**.

2 In the **Notification Users** section, select the user click **Edit User**.

3 Modify the settings in the **Add Notification User** dialog box as needed.

4 Click **OK** to save the settings.

Deleting a Notification User

To delete a notification user

1 Go to **Admin > SNMP Settings > Notification Setting**.

2 In the **Notification Users** section, click **Delete User**.

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

Adding a Notification Agent

The **Add Notification Agent** dialog box lets you add an SNMP agent to the RealPresence Access Director system, specifying what kinds of notifications it sends and to whom. To limit the effect on system performance, a maximum of eight agents may be defined.

To add an SNMP notification agent

1 Go to **Admin > SNMP Settings > Notification Setting**.

2 In the **Notification Agents** section, click **Add Agent**.

3 Configure the settings in the **Add Notification Agent** dialog box.

Field	Description
Notification Setting	
Notification Agents	Lists the notification agents that have been created. The system supports up to eight notification agents. The icon to the left of each entry indicates whether that agent is enabled.
Enable agent	Enables the notification agent defined below. Clearing this check box lets you stop using this agent without deleting it.
Transport	The transport protocol for SNMP communications to the host receiver (TCP or UDP).
Address	The IP address of the host receiver (the SNMP manager to whom this agent sends notifications).
Port	Specify the port that the RealPresence Access Director system will use to send notifications. By default, the system uses port 162.
Notification type	The type of notification that this agent sends to the notification receiver: • Inform — The agent sends an unsolicited message to a notification receiver and expects/requires the receiver to respond with a confirmation message. Introduced with SNMP version 2c, this option is not supported by network management systems that only support SNMP version 1. • Trap—The agent sends an unsolicited message to a notification receiver and does not expect/require a confirmation message.
SNMP version	The version of SNMP supported (v2c or v3).
Security user	For SNMPv3, specifies the security name required to access a monitored MIB object.

4 Click **OK**.

The agent appears in the **Notification Agents** list.

Editing a Notification Agent

To edit a notification agent

1. Go to **Admin > SNMP Settings > Notification Setting**.
2. In the **Notification Agents** section, select the agent to edit.
3. Click **Edit Agent**.
4. Modify the settings in the **Edit Notification Agent** dialog box as needed.
5. Click **OK** to save the settings.

Deleting Notification Agents

To delete a notification agent

1. Go to **Admin > SNMP Settings > Notification Setting**.
2. In the **Notification Agents** section, select the agent to delete.
3. Click **Delete Agent**.
4. Click **Yes** to confirm the deletion.

Downloading MIBs

The following table describes the MIBs that are available on the RealPresence Access Director system. You can download any of them from the **SNMP Settings** page. See To download a MIB on page 99.

Name	Description
INET-ADDRESS-MIB	A definition file for standard conventions included for reference.
polycom-access-management	The RealPresence Access Director system-specific MIB definition.
POLYCOM-BASE-MIB	Base MIB for Polycom products.
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.

Polycom recommends that you view MIB files with a MIB viewer application.

To download a MIB

1. Go to **Admin > SNMP Settings**.
2. Under **Actions**, click **Download MIBs**.
3. Select the MIB and click **Download**.

   The **Save As** window displays.
4. Navigate to where you want to save the MIB file locally and click **Save**.
5. Click **Close** to close the File Download window, then click **OK**.

Configuring History Retention Settings

The History Retention Settings can be configured to specify when the system purges call and registration history data. According to the values you specify for retention, the system purges the oldest registration history, call history, and registration signaling message records when:

- the number of records exceeds the maximum number to retain.
- the records have been stored for the maximum number of days.

When the system purges call history or registration history records, all of the associated data is also purged, including call events, call properties, and registration signaling events.

Some types of call signaling messages are not recorded in call history:

- SIP: OPTION, INFO

The following table describes the fields on the **History Retention Settings** page.

Field	Description
Enable recording of registration history	Enables the system to retain registration history records. Default: Enabled
Registration history records to retain	The number of registration history records the system retains before purging the oldest records. Default: 250,000 Range: 50,000 – 500,000
Registration signaling message records to retain	The number of system registration signaling message records the system retains before purging the oldest records. Default: 1,000,000 Range: 10,000 – 1,000,000
Enable recording of registration refresh	Enables the system to retain SIP registration refresh and H.323 lightweight Registration Request (RRQ) records. Default: Disabled

Field	Description
Call history records to retain	The number of call history records the system retains before purging the oldest records. Default: 250,000 Range: 50,000 – 500,000
History record purge interval	How often the system checks the number of registration and call history records to see if they exceed the maximums. When the maximum number of records to retain is reached, the system purges the excess. Default: Every 30 minutes Range: 5 – 1,440 minutes
The retention of history records according to time	The number of days that the system keeps system registration and call history records before purging the records that are older than the maximum number of days specified. Default: Every 90 days Range: 10 – 180 days

To configure history record retention

1. Go to **Admin > History Retention Settings**.
2. Specify the number of each type of record to retain in the system.
3. Specify how often you want the system to purge records in excess of those numbers.
4. Click **Update**.

   A dialog box informs you that the configuration has been updated.
5. Click **Set as Default** to keep the settings you entered as the default values.

Configuring Port Range Settings

You can configure port range settings to decrease the number of dynamic ports that need to be open on your enterprise's external and internal firewalls. A port range for a specific service indicates the number of ports that must be available to accommodate the number of calls for which your system is licensed.

After you have activated the license for your system, the RealPresence Access Director system automatically calculates the port ranges for your license. You can change port ranges as needed.

If you change any port ranges for dynamic source ports, you must also change the port range settings on your firewall. The port ranges in the RealPresence Access Director system must match the port ranges on the firewall.

When you specify a beginning port range number for signaling or media dynamic source ports, the RealPresence Access Director system automatically calculates the end port number for that service based on the number of calls on your system license.

You can configure ranges for the following ports:

- H.323 dynamic ports
- SIP dynamic source ports
- Access proxy dynamic source ports

  The access proxy feature is not related to the number of calls on a license and the full range of ports is available by default. You can specify both the beginning and end port numbers to limit the range for access proxy.
- External media ports
- Internal media ports

The table below summarizes general port information, the number of ports the RealPresence Access Director system reserves for each type of port, and an example port range on a system licensed for 1000 calls.

Service	Transport	Number of Ports Reserved	Beginning Port Number	Ending Port Number
H.323 dynamic ports	TCP	Number of licensed calls X 3	10001	13000
SIP dynamic source ports	TCP	Number of licensed calls X 2	13001	15000
Access proxy dynamic source ports	TCP	Variable Each dynamic mode client uses three ports (HTTPS provisioning, LDAP, and XMPP presence). Each RealPresence CloudAXIS Suite client, and RealPresence Content Sharing Suite client uses one port.	30001	60000
External media ports	UDP	Number of licensed calls X 10	20002	30001
Internal media ports	UDP	Number of licensed calls X 10	40002	50001

If you change the port range settings, the RealPresence Access Director system validates the new settings to ensure that no overlap occurs among any of the port range settings. Additionally, the system checks the port ranges to confirm the following:

- No end port number is greater than 60000.
- No beginning port number is less than 10000.
- No overlap occurs between the port ranges for TCP and no overlap occurs between the port ranges for UDP if they are on the same IP address.

To configure the port range settings

1. Go to **Admin > Port Range Settings**.

   If you have not activated your system license, the default settings for a 5-call trial license display.

2. Enter the beginning port number for the port range you want to change.

   The system automatically updates the port range values.

3. Click **Update** and confirm the changes.

   The system confirms that the update was successful.

User Management

The Polycom® RealPresence® Access Director™ system enables you to manage local user accounts. You can search for, add, edit, and delete user accounts as needed.

Working with Local User Accounts and User Roles

The RealPresence Access Director system provides user roles, each with its own set of privileges, to support administration and management of the system. When creating a local user account, you can assign one or more user roles to each user. The following table provides a brief overview of each user role.

Changing Your System Password

To change your system password

1. Go to **User > Users**.
2. Select your account from the list of users.
3. Under **Actions**, click **Edit**.
4. Enter your new password in the **Password** and **Confirm Password** fields.
5. Click **OK**.

Searching for a Local User Account

Both administrators and provisioners can search for local user accounts.

To search for a user account

1. Go to **User > Users**.
2. To reveal search filters, click  .
3. Enter search string parameters in any of the following fields as needed to refine your search:
   - **Search users**
   - **User ID**
   - **First name**
   - **Last name**
4. To search by a user's role, click the down arrow in the **Role** field and select the role.

5 Click **Search**.

- For a string search:

  The system attempts to match the string you entered against the beginning of the value for which you are searching. For example, if you enter ***sa*** in the **Search users** field, the system displays users whose first name, last name, or user ID begins with ***sa***.

- For a role search:

  The system displays all local user accounts that are assigned to the role that you selected.

Role	Description
Administrator	Performs system configuration, management, and ongoing system administration. The administrator has full privileges to operate the system.
Auditor	Views active calls, call history, and registration history, manages system log files, and uses traffic capture, ping, and traceroute to diagnose system issues.
Provisioner	Performs a subset of administrator responsibilities, such as partial configuration and services. Provisioners can facilitate daily activities, such as personnel changes and troubleshooting call issues, for large deployments.

The following topics provide details about user management options:

- Adding a Local User Account
- Editing and Deleting Local User Account Information on page 105

Adding a Local User Account

Only administrators can add user accounts.

To add a local user account

1 Go to **User > Users.**

2 Under **Actions**, click **Add**.

3 In **General Info**, complete the following fields:

Field	Description
First name	User's first name
Last name	User's last name
User ID	User's login name
Password	User's system login password
Confirm password	Repeat user's system login password

4 Click **Associated Roles** and select one or more roles for the new user.

5 Click  to add the roles to the **Selected roles** list.

Selecting user roles is optional. If you do not select a role, the system assigns **Auditor** as the default user role.

6 Click **OK**.

Editing and Deleting Local User Account Information

Only administrators can edit all information for user accounts. Both administrators and provisioners can edit their own passwords.

Only administrators can delete user accounts.

Be aware of the following before deleting a user account:

- When you delete an account, all of the account data is removed from the system.
- When you delete the account of a user who is logged into the system, the user is not affected by the deletion. The deletion is completed when the user logs out, and the user will not be able to log into the system again.
- One administrator account must always exist in the system; if the system has only one administrator account, it cannot be deleted.
- Administrators cannot delete their own accounts.

To edit user information

1 Go to **User > Users**.

2 Select a user account from the list.

3 Click **Edit**.

4 Revise the user information and role as needed.

5 Click **OK**.

To delete a user account

1 Go to **User > Users**.

2 Select a user account from the list.

3 Click **Delete**.

4 In the **Confirm Action** dialog box, click **Yes** to complete the action.

System Maintenance

The following topics describe maintenance functions for the Polycom® RealPresence® Access Director™ system:

- Upgrading the Software
- Shutting Down and Restarting the System
- Backing Up and Restoring

Upgrading the Software

The RealPresence Access Director system can be upgraded from the user interface. You can upload and install an upgrade file in one operation or upload an update file for later installation. Additionally, the roll back feature allows you to downgrade back to the previous version if necessary.

Only administrators can upgrade or roll back system software versions.

Polycom recommends that you download backup files before beginning an upgrade.

Upgrading and rolling back requires a system restart, which terminates active calls and logs all users out of the system.

After upgrading or rolling back, delete temporary Internet files and cookies from Internet Explorer before accessing the RealPresence Access Director system user interface. See Cannot Open RealPresence Access Director System User Interface on page 133.

Viewing Software Information

You can display information about the current software version in the following ways:

- Click **Help > About RPAD**.
- Go to **Maintenance > Software Upgrade**.

The **Software Upgrade** page displays the following system information:

- Current system and rollback versions
- Upgrade package details
- A history of upgrade and rollback operations for the system

Uploading an Upgrade Package File

You can upload only one upgrade package at a time. If a package has already been uploaded and you attempt to upload another, the system notifies you that an upgrade package has already been uploaded and asks whether you want to replace it. You can then cancel the current operation or continue with the upload action and replace the previously uploaded package.

If the upgrade requires a new license activation key code or codes, obtain and install them as described in Obtaining an Activation Key Code on page 22.

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

To upload a package file for later installation

1. Go to **Maintenance > Software Upgrade**.
2. Under **Actions**, click **Upload**.
3. Select the upgrade package file, and click **Open**.

   The **File Upload** dialog box indicates when the upload is complete.
4. Click **Close**.

   The **Operation History** displays the status of the upload. Additionally, **Upgrade Package Details** displays information about the upgrade file.

Installing an Uploaded Package File

When you upload an upgrade package, the **Upgrade** option displays under the **Actions** menu.

The upgrade installation procedure automatically creates a backup file, which you can use to roll back to the previous version or the last applied upgrade, if necessary.

Upgrading does not delete previous backup files from the system. See the **Backup and Restore** feature to determine the system version of a backup file.

Always read the upgrade release notes before installing an upgrade.

Upgrades require a system restart, which terminates active calls and logs all users out of the system.

To install an uploaded upgrade package file

1. Go to **Maintenance > Software Upgrade**.
2. Under **Actions**, click **Upgrade**.
3. Click **Yes** to confirm the system upgrade.

   The system notifies you that the upgrade is starting.

4 Click **OK** to log out.

The user interface closes during the upgrade process.

5 After the upgrade is complete, open a new browser window and access the RealPresence Access Director system user interface.

The End-user License Agreement displays.

6 Click **Accept** to advance to the log-in page.

The **System version** should indicate the version number of the upgrade.

7 Log into the system and go to **Maintenance > Software Upgrade**.

8 Review the **System version** and **Operation History** to confirm the upgrade was successful.

Uploading and Upgrading at the Same Time

To upload and install an upgrade package file

1 Go to **Maintenance > Software Upgrade.**

2 From the **Actions** menu, click **Upload and Upgrade**.

3 Navigate to the upgrade package file, and click **Open**.

After the upload is complete, the upgrading procedure begins automatically and the user interface closes.

4 After the upgrade is complete, open a new browser window and access the RealPresence Access Director system user interface.

The End-user License Agreement displays.

5 Click **Accept** to advance to the log-in page.

The **System version** should indicate the version number of the upgrade.

6 Log into the system and go to **Maintenance > Software Upgrade**.

7 Review the **System version** and **Operation History** to confirm the upgrade was successful.

Rolling Back to the Previous Software Version

The **Software Upgrade** page **Actions** menu displays the **Roll Back** option if a downgrade package file is available. Additionally, **Version Information** displays the **Rollback version** number.

As a precaution, Polycom recommends that you download a recent backup file before beginning a roll back procedure. Rolling back restores the database to its state before the last applied upgrade, so data may be lost.

To roll back the system to the previous version

1 Go to **Maintenance > Software Upgrade**.

2 Under **Version Information**, verify that the rollback version is correct.

3 From the **Actions** menu, click **Roll Back**.

4 In the **Confirm Action** dialog box, click **Yes**.

The system notifies you that the roll back is starting.

5 Click **OK**.

The user interface closes during the rollback process.

6 After the rollback is complete, open a new browser window and access the RealPresence Access Director system user interface.

The **System version** should be the rollback version.

7 Log into the system and go to **Maintenance > Software Upgrade**.

8 Review the **Rollback version** and **Operation History** to confirm the rollback was successful.

Shutting Down and Restarting the System

Only administrators can shut down and restart the system.

Use caution when shutting down or restarting the system. Both of these actions terminate active calls and log all users out of the system.

To shut down the system

1 Go to **Maintenance > Shutdown and Restart**.

2 Click **Shut Down**.

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

All active calls are terminated and users are logged out.

To restart the system

1 Go to **Maintenance > Shutdown and Restart**.

2 Click **Restart**.

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

All active calls are terminated and users are logged out. Typically, service is restarted after about five minutes.

Backing Up and Restoring

The RealPresence Access Director system's **Backup and Restore** page lets you:

- Manually create a backup of the basic system configuration and database files at any time. System configuration information includes OS network, hostname, and IP route.

- Download backup files from the RealPresence Access Director server to a local machine for safekeeping.
- Upload backup files from a local machine to the RealPresence Access Director server.
- Remove a backup file from the system server.
- Restore the RealPresence Access Director system configuration from a specific backup file. The backup file used to restore the system configuration settings must be from the same version of the system as the version currently in use.

Note

Polycom strongly recommends that you:

- Download backup files regularly for safekeeping.
- Restore from a backup only when there is no activity on the system. Restoring terminates all calls and restarts the system.

To view general information about backup files

» Go to **Maintenance > Backup and Restore**.

The information below displays for each backup file:

Field	Description
Creation Date	The date and time when the backup file was created.
Name	The name of the backup file. The system automatically generates the name when you create a new backup file. The file extensions for backup files is **.image**.
Size	The size of the backup file.
System Version	The version of the RealPresence Access Director system in use when the backup file was created.

To create a new backup file

1. Go to **Maintenance > Backup and Restore**.
2. Under **Actions**, click **Create New**.

   The system creates a new backup file and displays it in the list of backup files.

Log files are not included in backup files.

To upload a backup file to the system server

1. Go to **Maintenance > Backup and Restore**.
2. Under **Actions**, click **Upload**.

3 Select the backup file to upload to the RealPresence Access Director server and click **Open**.

The progress of the file upload displays.

4 Click **Close** when the upload is complete.

To restore the system from a backup file

1 Go to **Maintenance > Backup and Restore**.

2 If you haven't already done so, upload the backup file to use to restore the system.

The backup file used to restore the system must be from the same version of the system as the version currently in use.

3 Select the file from the list of backup files.

4 Under **Actions**, click **Restore Selected**.

5 In the **Confirm Action** dialog box, Click **Yes** to restore the system from the backup file you selected.

To remove a backup file

1 Go to **Maintenance > Backup and Restore**.

2 Select the backup file to remove from he RealPresence Access Director server.

3 Under **Actions**, click **Remove Selected**.

4 In the **Confirm Action** dialog box, Click **Yes** to remove the backup file you selected.

System Diagnostics

The Polycom® RealPresence® Access Director™ system provides several network and system status commands that help to ensure optimum performance of the system. Additionally, log files provide detailed system information.

The following topics describe the commands and diagnostic tools you can use to assess system performance:

Using Active Call

To view details about active calls

1. Go to **Diagnostics > Active Call**.

   The system displays the following call details:

   - Start Time
   - Originator
   - Destination
   - Bandwidth (kbps)
   - Signaling

2. To change how often the system updates the details, click **Refresh: Every 15 seconds** and select the refresh interval.

Auditing Call History

The call history function lets you view detailed records of calls and call signaling events.

The historical data that is available depends on the settings you configure for history retention. See Configuring History Retention Settings on page 99.

Searching for Call Records

The search pane above the call list lets you find calls that match the criteria you specify. The search feature supports a wildcard (*) search for the **Originator** and **Dial string** parameters.

The **Start After** and **Start Before** settings are always active and define the time range during which the calls you are searching for began. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

To search for calls

1. Go to **Diagnostics > Call History**.
2. Enter the search criteria as described in the following table:

Column	Description
Start after	The time after which the call began.
Start before	The time before which the call began.
Signaling type	SIP or H.323
Originator	The originating device's display name, name, alias, or IP address (in that order of preference), depending on what it provided in the call signaling.
Dial string	Dial string sent by originator, when available.

3. Click **Search**.

   The search results list the calls in the time range you specified. If there are more than 500, the first page lists the first 500, and the arrow buttons below the list let you view other pages.

Viewing Call Details

After you search for call history records, you can view details for a specific call record.

To view call information

1. Go to **Diagnostics > Call History** and complete a search for call history records.

2 From the search results, select a call and click **Show Call Details** under the **Actions** list. **Call Info** displays the following detailed information about the selected call.

Category	Information	Value
Call Info	Call status	Active or ended. A call becomes active after the RealPresence Access Director system receives the first call request and routes the call to the next hop address.
	Start time	The time the call began (first signaling event).
	End time	The time the call ended (session closed). This field is blank if the call is active.
	Duration	Duration of the call in minutes.
	Signaling	SIP or H.323
Originator	Call ID	The unique identifier for the call.
	From	The originating endpoint's display name, name, alias, or IP address.
	To	The destination endpoint's display name, name, alias, or IP address.
	Dialed string	The dial string sent by the originator.
	IP address	The IP address from which the RealPresence Access Director system receives SIP INVITE and H.323 SETUP messages.
Destination	Call ID	The unique identifier for the call.
	From	The originating endpoint's display name, name, alias, or IP address.
	To	The destination endpoint's display name, name, alias, or IP address.
	Dialed string	The dial string sent by the originator.
	IP address	The IP address to which the RealPresence Access Director system sends SIP INVITE and H.323 SETUP messages.

To view call event details

1 Go to **Diagnostics > Call History** and complete a search for call history records.

2 From the search results, select a call and click **Show Call Details** under the **Actions** list.

3 Select **Call Events** to display all signaling events for the selected call.

To view subscription event details

1 Go to **Diagnostics > Call History** and complete a search for call history records.

2 From the search results, select a call and click **Show Call Details** under the **Actions** list.

3 Select **Subscription Events** to display all subscription events for the selected call.

Auditing Registration History

When a SIP or an H.323 endpoint makes a call through the RealPresence Access Director system, the system registers the endpoint device. Each device registration is identified by a Universally Unique Identifier (UUID), which allows details and events of a registration to be grouped. The **Registration History** function provides access to information about the registered devices.

Searching for Registration Records

The search pane above the list of registrations lets you find device registrations that match the criteria you specify. The search feature supports a wildcard (*) search for the **Alias** parameter.

The **Start After** and **Start Before** settings are always active and define the time range during which the registrations you are searching for began. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

To search for device registrations

1 Go to **Diagnostics > Registration History**.

2 Enter the search criteria as described in the following table:

Column	Description
Start after	The time after which the call began.
Start before	The time before which the call began.
Signaling type	SIP or H.323
Alias	The originating device's alias.
IP address	The originating device's IP address.

3 Click **Search**.

The search results list the registration records for the time range you specified. If there are more than 500, the first page lists the first 500, and the arrow buttons below the list let you view other pages.

Viewing Registration Details

After you search for device registration records, you can view details for a specific registration record.

To view registration information

1 Go to **Diagnostics > Registration History** and complete a search for device registrations records.

2 From the search results, select a registration record and click **Show Registration Details** under the **Actions** list. **Registration Info** displays the following detailed information about the selected registration record.

Column	Description
Signaling	SIP or H.323
Name	The name of the registered device.
Alias	The device's alias.
Address	The device's IP address and port number.
Start Time	The time and date that the device registered.
End Time	The time and date that the device's registration ended (blank if the device is still registered).

To view registration event details

1 Go to **Diagnostics > Registration History** and complete a search for device registrations records.

2 From the search results, select a registration record and click **Show Registration Details** under the **Actions** list.

3 Select **Registration Events** to display the event information about the selected registration record.

Event	Event Details	Description
Registration begin	Alias	**SIP** Specifies the SIP URI in the header of the SIP REGISTER message. **H.323** Lists all aliases of a client terminal included in the RRQ message.
	Signaling type	SIP or H323
	Direction	Specifies if the registration was inbound or outbound.

Event	Event Details	Description
Signaling	Event type	Indicates if the event was a request or a response, and the direction of the response (inbound or outbound).
	Far end	The IP address and port of the far end from which the system received a signaling message
	Summary	**SIP** Specifies the SIP request method or response code. **H.323** Identifies the registration request, reject, or confirm messages.
	Details	The text of the event message.
Registration end	Reason	Specifies if the registration event was terminated by the remote endpoint or by the RealPresence DMA system.

Working with System Log Files

The RealPresence Access Director system uses the Syslog standard to create system log files that contain detailed information about system modules. All log files are stored locally and on remote syslog servers to enable tracking and analyzing system information, including any security events.

Syslog generates the structured data, message IDs, and other dynamic log data in a standardized, user-friendly format. It also filters the logs to the syslog-ng log management infrastructure. Syslog-ng stores the logs as local log files and forwards them to remote syslog servers.

For more information on configuring the log files settings for your system, see Configuring Log Settings on page 88.

The table below describes the different types of system log files available in the RealPresence Access Director system.

Name	Contents of Log
webAdmin	Information about the Web user interface and related operations.
dbAccess	All operations for SIP, H323, and access proxy to fetch configuration parameters.
license	License information, such as new calls, SIP and H.323 active call numbers and bandwidth, adjusted bandwidth, bandwidth limitation, and number of licensed calls.
audit	Call history and registration history information.

Name	Contents of Log
utility	Information on all system utility modules, such as scheduling and date utilities.
sipService	Information about SIP calls, such as caller, endpoint recipient, contact, user agent, max forwards, expiration, route, path, and content length.
h323Service	Information about H.323 calls such as handling messages, call state changes, media resource use, license use, bandwidth use, and service status. Log contents are dependent on the Logging Level. See Configuring Log Settings on page 88.
mediaTraversal	Information on a call's media session, such as start, stop, or restart, media path information logged as a route entry Allocation information for a call's media ports, such as reserving or releasing a pair of RTP & RTCP ports; includes the internal and external network adapter information for media use.
accessProxy	Information about an endpoint's message exchanges with the internal server, including login, contact searches, presence status, source IP address and port, destination IP address and port, message protocol, and content details (if the logging level is DEBUG). See Configuring Log Settings on page 88 for details on setting the logging level.
serviceController	Information on the service controller module, which controls other system components.
snmp	Information recorded about the SNMP service, including SNMP GET requests received and trap messages sent.
tunnel	Information about tunnel communication, including tunnel status and the results of enabling or disabling the tunnel.

These topics provide details on working with system log files:

- Viewing the Disposition for SIP and H.323 Calls on page 118
- Downloading Log Files on page 119
- Deleting Log Files on page 120
- Rolling Log Files on page 120

Viewing the Disposition for SIP and H.323 Calls

The RealPresence Access Director system logs disposition information for SIP and H.323 calls. You can view this information in the **sipService** and **h323Service** logs.

The tables below describe the different dispositions.

SIP Dispositions

Disposition	Description
Accept	RealPresence Access Director system license controller and SIP module accepts a new SIP call
Forward	RealPresence Access Director system SIP module forwards a SIP request/response
Reject	RealPresence Access Director system SIP module rejects a SIP call
Discard	RealPresence Access Director system SIP module discards a SIP request/response
Release	RealPresence Access Director system SIP module releases a SIP call session

H.323 Dispositions

Disposition	Description
Forward	RealPresence Access Director system H.323 module forwards an H.323 message
Auto-response	RealPresence Access Director system H.323 module automatically responds
Auto-request	RealPresence Access Director system H.323 module automatically sends a request
Release	RealPresence Access Director system H.323 module releases an H.323 call session

Downloading Log Files

To view the list of system log files

1. Go to **Diagnostics > System Log Files**.
2. In the **Filter** list, click the arrow to select either **Active logs** or **Archive logs**.

   The log files list includes the following information.

Column	Description
Time	Date and time that the log file was created.
Host	Hostname of the RealPresence Access Director system server.

Column	Description
Filename	Name of the log file. All log files with the extension *.log.(number) are rolling logs. For example, when the size of **webAdmin.log** reaches the maximum log file size, the log file will be rolled up to **webAdmin.log.1** and it will keep rolling up to **webAdmin.log.10**. After the maximum file size for *.log.10 is reached, the system will start rolling logs again by overwriting *.log.1.
Size	Size of the file in megabytes.

To download a system log file

1. Go to **Diagnostics > System Log Files**.
2. In the **Filter** list, click the arrow to select either **Active logs** or **Archive logs**.
3. Select the log file to download.
4. Under **Actions**, select **Download Logs**.
5. In the **Save As** dialog box, select a location, and choose **Save**.

Deleting Log Files

To delete a system log file

1. Go to **Diagnostics > System Log Files**.
2. In the **Filter** list, click the arrow to select either **Active logs** or **Archive logs**.
3. Select the log file to delete.
4. Under **Actions**, select **Delete Logs.**
5. In the **Confirm Action** dialog box, Click **Yes** to delete the log file.

Rolling Log Files

To roll an active log file into an archive file

1. Go to **Diagnostics > System Log Files**.
2. Select the log file to roll.
3. Under **Actions**, select **Roll Logs**.

   A message displays to confirm that the rolled log file was created in the archive directory.
4. Click **Yes** to download the log file.
5. In the **Save As** dialog box, select a location, and choose **Save**.
6. Click **Close** when the download is complete.

Running Traffic Capture

Traffic Capture uses Linux tcpdump commands to capture packets received or sent by the network interfaces on your system. The traffic capture generates a packet capture (.pcap) file that contains the network traffic information.

The packet capture file shows the communication flow of traffic proxied by the RealPresence Access Director system, and includes the source and destination IP addresses. For example, when a remote user signs into Polycom RealPresence Desktop, the capture file shows the remote endpoint calling into the RealPresence Access Director system and the RealPresence Access Director system proxying the registration request to RealPresence Resource Manager system.

The capture file shows media packet information in a slightly different way. The captured media packets display twice in the capture file as being to or from the internal LAN-side video system's IP address and the external video system's IP address. Incoming media packets are captured after the RealPresence Access Director system has proxied the call. Therefore, the destination IP address of an incoming media packet is modified to display the target endpoint’s IP address instead of the RealPresence Access Director system’s IP address. The destination IP address and source IP address of an outgoing packet correctly display the traffic flow through the RealPresence Access Director system.

To capture packets per individual network interface, contact Polycom Global Services for support.

To run Traffic Capture

1. Go to **Diagnostics > Traffic Capture**.
2. Select the type of packet data to capture.
3. Select **All (including media packet)** to capture SIP, H.323, access proxy, and media packets.
4. Click **Capture** to start the packet data capture.
5. Click **Stop** to stop the capture.

   The RealPresence Access Director system generates a packet capture file with the `.pcap` extension and prompts you to download the file from **Diagnostics > System Log Files**.

To download a packet capture file

1. Go to **Diagnostics > System Log Files** and select the `.pcap` file to download.
2. Under **Actions**, click **Download Logs** and select a location to save the file.

   The system notifies you when the download is complete.

Running Ping

Use **Ping** to verify that the RealPresence Access Director system can communicate with another device on the network.

To run Ping on a network device

1. Go to **Diagnostics > Ping**.
2. Enter an IP address or hostname and click **Ping**.

   The system displays the results of the command.

Running Traceroute

Use **Traceroute** to view these details:

- The route that the RealPresence Access Director system uses to reach the address you specify
- The latency (round trip) for each hop.

To run Traceroute on an address

1. Go to **Diagnostics > Traceroute**.
2. Enter an IP address or hostname and click **Trace**.

   The system displays the results of the command.

Using Polycom Utilities

If your RealPresence Access Director system is shipped with a Dell R620 server, the system shipment includes a USB flash drive labeled *Polycom Utilities* that includes server diagnostic utilities. Please note:

- You should use these server diagnostic utilities only under the direction of Polycom Global Services at support.polycom.com.
- You will need a monitor and USB keyboard to use these utilities.

Troubleshooting

This section provide information to assist in ensuring optimum performance of the Polycom® RealPresence® Access Director™ system.

Refer to the topics below for the recommended troubleshooting actions for specific issues:

For additional information on troubleshooting, see the *Polycom RealPresence Access Director Deployment Guide*, available at support.polycom.com.

Remote Client Sign In Failed

Possible Reasons	Recommended Actions

Access proxy error	In the RealPresence Access Director system
	• Go to the **Services Status** pane on the Dashboard and check whether access proxy is running. If it has stopped running, complete the following steps:
	In the RealPresence Resource Manager system
	• Do one of the following:
	  ⮝ In version 7.1.1, go to **Admin > Troubleshooting Utilities > Test Network > Ping**.
	  ⮝ In version 8.0, go to **Admin > Maintenance > Troubleshooting Utilities > Test Network > Ping**.
	• Check whether the RealPresence Access Director system is accessible.
	On the inside firewall
	• Check the firewall policy to determine if the HTTPS, LDAP, and XMPP ports all permit calls from untrust to trust zone. Default values are:
	  ⮝ HTTPS: TCP 443
	  ⮝ LDAP: TCP 389
	  ⮝ XMPP: TCP 5222
	In the RealPresence Access Director system
	• Wait 10 minutes, then check whether access proxy is running.
	• Restart the system if access proxy is still not running.

Firewall configuration error	On the outside firewall
	• Check whether the public IP address of the RealPresence Access Director system is mapped to its internal signaling IP address.
	• Check the firewall policy to determine if HTTPS, LDAP and XMPP ports are all permitted from untrust to trust zone. Default values are:
	  ⮝ HTTPS: TCP 443
	  ⮝ LDAP: TCP 389
	  ⮝ XMPP: TCP 5222

Possible Reasons	Recommended Actions
Certificate check fails	In the RealPresence Access Director system • Go to **Configuration > Access Proxy Settings**. • Select **HTTPS** and click **Edit** to check whether **Require client certificate from the remote endpoint** or **Verify certificate from internal server** is selected. If selected, disable them and try to log in again. If you can log in after disabling these two settings, your certificates are not installed correctly. • Check whether the certificates on the RealPresence Access Director system and the RealPresence Resource Manager system are trusted by each other, and whether certificates on the RealPresence Access Director system and remote clients are trusted by each other. • Enable **Require client certificate from the remote endpoint** and **Verify certificate from internal server** after checking that the certificates are installed correctly • Repeat for each protocol as necessary.
No network connection on Polycom® RealPresence® Mobile	Check the wireless connection on the mobile device
Sign-in server address error	On the remote client, confirm that the sign-in server address is the public address of the RealPresence Access Director system.

Site configuration error	In the RealPresence Resource Manager system
	• Do one of the following:
	  ◦ In version 7.1.1, go to **Admin > Topology > Sites**.
	  ◦ In version 8.0, go to **Admin > Network topology > Sites**.
	• Check whether the signaling IP address of the RealPresence Access Director system is included in the subnets.

User configuration error	In the RealPresence Resource Manager system • Go to **User > Users**. • Check whether the user that is signed in can be found in a search of the local user list or in the LDAP user list.

Licensed Call Number is 0

Possible Reasons	Recommend Actions
Trial period expires	Purchase a license. In the RealPresence Access Director system • Go to **Maintenance > License > Activation key** and enter the new key. • Click **Update**.
License is invalid due to system time being changed.	If you have purchased a license, in the RealPresence Access Director system • Go to **Maintenance > License > Activation key** and re-enter the license activation key. • Click **Update**. If you have a trial license, you must re-install the RealPresence Access Director system server to generate a new trial period license. **CAUTION** If you reinstall the system server, all manually configured or provisioned settings will be lost.

SIP Registration Failed

Possible Reasons	Recommend Actions
SIP component not running	In the RealPresence Access Director system • Go to the **Services Status** pane on the Dashboard and check whether **SIP** is running. If it is not running complete the following steps: • Go to **Configuration > SIP and H.323 Settings**. • Check whether SIP is enabled. If not, select **Enable SIP signaling**. • Restart the system if SIP is still not running.

Possible Reasons	Recommend Actions
SIP configuration error	In the RealPresence Access Director system • Go to **Configuration > SIP and H.323 Settings**. • Check the value of **Registration refresh interval**. • Check whether the system listens on the SIP port and protocol that the client uses. In the RealPresence DMA system • Check whether the **Minimum SIP registration interval** of the SIP registrar server allows the registration refresh interval from the RealPresence Access Director system. • Check whether the SIP registrar server listens on the configured SIP port and protocol used by the RealPresence Access Director system.
SIP server address error	On the remote client • Check whether the SIP registrar server address is the public address of the RealPresence Access Director system.
TLS port error	In the RealPresence Access Director system When TLS is selected as the transport protocol between the RealPresence Access Director system and the RealPresence DMA system, ensure that the port is 5061, not 5060.

Site configuration error	In the RealPresence Resource Manager system
	• Do one of the following:
	  ⅄ In version 7.1.1, go to **Admin > Topology > Sites**.
	  ⅄ In version 8.0, go to **Admin > Network topology > Sites**.
	• Check whether the SIP registrar server address for remote clients is the public address of the RealPresence Access Director system.

Authentication error	In the RealPresence DMA system • **Go to Admin > Local Cluster > Signaling Settings > SIP Settings**. • Check whether the SIP registrar server enables SIP authentication and ensure that the client uses the correct SIP account.

Possible Reasons	Recommend Actions

Firewall configuration error	In the RealPresence DMA system
	• Go to **Maintenance > Troubleshooting Utilities > Ping**.
	• Check whether the RealPresence Access Director system is accessible.
	On the inside firewall
	• Check the firewall policy to determine if SIP ports are all permitted from untrust to trust zone. Default values are:
	  ⅄ TCP: 5060, 5061
	  ⅄ UDP: 5060
	On the outside firewall
	• Check whether the public signaling IP address of the RealPresence Access Director system is mapped to its internal signaling IP address.
	• On both outside and inside firewall, check the firewall policy to determine if SIP ports are permitted from untrust to trust zone.

Certificate install error	If the client uses SIP TLS, check whether the certificates on the RealPresence Access Director system are correctly installed.

SIP Call Failed

Possible Reasons	Recommend Actions
Endpoint registration error	On the caller and callee endpoints • Check whether both the caller and the endpoint being called are registered. • Unregister and reregister the endpoint and call again.

Service network setting error	In the RealPresence Access Director system
	• Go to **Admin > Network Settings > Service network setting**.
	• If the RealPresence Access Director system is deployed behind a firewall, check the **Outside Firewall/NAT** settings to ensure the following:
	  ⅄ **Deployed behind Outside Firewall** is selected.
	  ⅄ **Signaling relay address** and **Media relay address** contain the public address of the RealPresence Access Director system mapping on a firewall.

License limitation	In the RealPresence Access Director system • Go to the **License Status** pane on the Dashboard. • Check whether the **Maximum Allowed Calls** have been reached.
RealPresence DMA system configuration error	In the RealPresence DMA system, determine if the dial rule configurations are correct.

Possible Reasons	Recommend Actions
SIP ALG	• Check whether SIP ALG is enabled on the home NAT and firewall. • Disable SIP ALG and try the call again.
Bandwidth limitation:	Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system. • Go to **Configuration > Media Traversal Settings**. • Increase bandwidth limitation values. • Try the call again.

H323 Call Failed

Possible Reasons	Recommend Actions
H.323 component not running	In the RealPresence Access Director system • Go to the **Services Status** pane on the Dashboard. • Check whether H.323 is running. If it is not running complete the following steps: • Go to **Configurations > SIP and H.323 Settings**. • Check whether H.323 signaling is enabled. If not, select **Enable H.323 signaling**. • Restart the system if H.323 is still not running.
Callee registration error	On the callee endpoint, check whether the endpoint is registered with the gatekeeper.

H.323 configuration error	In the RealPresence Access Director system
	• Go to **Admin > Network Settings > Service network setting**.
	• If the RealPresence Access Director system is deployed behind a firewall, check the **Outside Firewall/NAT** settings to ensure the following:
	  ⅄ **Deployed behind Outside Firewall** is selected.
	  ⅄ **Signaling relay address** and **Media relay address** contain the public address of the RealPresence Access Director system mapping on a firewall.
	• Go to **Configuration > SIP and H.323 Settings > H.323 Settings**.
	• Make sure that all RealPresence DMA system and internal endpoint subnets are included in the CIDR address.

License limitation	In the RealPresence Access Director system • Go to the **License Status** pane on the Dashboard. • Check whether the **Maximum Allowed Calls** have been reached.

Possible Reasons	Recommend Actions
Network issue between the RealPresence Access Director system and the gatekeeper	In the RealPresence DMA system • Go to **Maintenance > Troubleshooting Utilities > Ping** and check whether the RealPresence Access Director system is reachable.
H.225 port error	In the RealPresence Access Director system • Go to **Configuration > SIP and H.323 Settings**. • Check whether the RealPresence Access Director system and the endpoint use the same H.225 signaling port, which is 1720 by default.
Firewall configuration error	On the outside firewall • Check whether the public signaling IP address of the RealPresence Access Director system is mapped to its internal IP address. On the outside and inside firewall • Check the firewall policy to determine if H.323 ports are permitted from untrust to trust zone. ⮝ Default H.323 port is 1720.
RealPresence DMA system configuration error	In the RealPresence DMA system, determine if the dial rule configurations are correct.
H.323 ALG	• Check whether H.323 ALG is enabled on the home NAT and firewall. • Disable H.323 ALG and try the call again.
Bandwidth limitation	Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system. • Go to **Configuration > Media Traversal Settings**. • Increase bandwidth limitation values. Try the call again.

VMR Call Failed

Possible Reasons	Recommend Actions

Call signaling error	• Check whether a SIP or H.323 P2P call works correctly.
	  ⮝ If so, the RealPresence Access Director system, the RealPresence DMA system, the endpoint, and the firewall configurations are all correct.
	  ⮝ If a P2P call does not work correctly, see the possible reasons in SIP Call Failed on page 128 and H323 Call Failed on page 129.

Possible Reasons	Recommend Actions
VMR configuration error	In the RealPresence DMA system, determine if the VMR number is correct.
RealPresence DMA system configuration error	In the RealPresence DMA system, determine if the dial rule configurations are correct.

No Audio, Video, or Content

Possible Reasons	Recommend Actions
Media relay component error	In the RealPresence Access Director system • Go to the **Services Status** pane on the Dashboard. • Check whether the **Media Relay** is running. • Restart the system if Media Relay stops working.
Endpoint error	• Check whether the audio is mute on the endpoint. • Check whether the camera works correctly on the endpoint.
Service network setting	In the RealPresence Access Director system • Go to **Admin > Network Settings > Service network setting**. • If the RealPresence Access Director system is deployed behind a firewall, check the **Outside Firewall/NAT** settings to ensure the following: ➢ **Deployed behind Outside Firewall** is selected. **Signaling relay address** and **Media relay address** contain the public address of the RealPresence Access Director system mapping on a firewall.
BFCP over UDP for content	• The RealPresence Access Director system supports BFCP over UDP. • Make sure the endpoint or MCU supports BFCP over UDP as well.
SIP or H.323 ALG	• Check whether SIP or H.323 ALG is enabled on the home NAT and firewall. • Disable SIP or H.323 ALG and try the call again.
Firewall configuration error	On the outside firewall, • Check the firewall policy to determine if external media ports are permitted from untrust to trust zone. ➢ –UDP: 20001-40000 On the inside firewall • Check the firewall policy to determine if internal media ports are permitted from trust to untrust zone. ➢ –UDP: 40001-60000

Failed to Connect to RealPresence Resource Manager System

Possible Reasons	Recommend Actions
Login name/password error	In the RealPresence Access Director system • Go to **Admin > Polycom Management System**. • Check whether the login name and password are correct.

Network issue between the RealPresence Access Director system and the RealPresence Resource Manager system	In the RealPresence Resource Manager system
	• Do one of the following:
	  ◦ In version 7.1.1, go to **Admin > Troubleshooting Utilities > Test Network > Ping**.
	  ◦ In version 8.0, go to **Admin > Maintenance > Troubleshooting Utilities > Test Network > Ping**.
	• Check whether the RealPresence Access Director system is accessible.

Certificate check fails	In the RealPresence Access Director system • Go to **Admin > Polycom Management System**. • Check whether **Verify certificate from internal server** is selected. • If selected, disable the field and try the call again.
Certificate install error	In the RealPresence Access Director system • Go to **Admin > Polycom Management System**. • Check whether **Verify certificate from internal server** is selected. • If selected, check whether the certificates on the RealPresence Access Director system and the RealPresence Resource Manager system are correctly installed.

Site configuration error	In the RealPresence Resource Manager system
	• Do one of the following:
	  ◦ In version 7.1.1, go to **Admin > Topology > Sites**.
	  ◦ In version 8.0, go to **Admin > Network topology > Sites**.
	• Select the site that you're troubleshooting and click **Edit**.
	• In General Info, check whether **Site with RPAD** is selected.
	• Click **Subnets** and check whether the internal signaling IP address of the RealPresence Access Director system is listed.

User configuration error	In the RealPresence Resource Manager system • Go to **User > Users**. • Check whether the login name of the user is in the user list.

Cannot Open RealPresence Access Director System User Interface

Possible Reasons	Recommend Actions

Internet Explorer browser cache issue when upgrading from version 2.x to version 3.0, then rolling back to version 2.x.	• Close and re-open the Internet Explorer browser
	• Access the RealPresence Access Director system user interface. If you are still unable to open the interface, delete the Internet Explorer cache files.
	  ⅄ In Internet Explorer, go to **Tools > Internet Options > General > Browsing History > Delete** and select **Temporary Internet files** and **Cookies**.
	  ⅄ Click **Delete**, then open the user interface.
	• Refer to Internet Explorer or Windows help if you do not have the necessary account permissions to delete the cache files.