



2.0 | November 2012 | 3725-78703-001A

Polycom[®] RealPresence[®] Access Director[™] System Administrator's Guide



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 property of their respective owners. .



Java is a registered trademark of Oracle 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 Access Director system end-user license agreement (EULA).

The EULA is included in the release notes document for your version, which is available on the Polycom Support page for the system.

© 2012 Polycom, Inc. All rights reserved.

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

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

As between the parties, Polycom, Inc., retains title to and ownership of all proprietary rights with respect to the software contained within its products. The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g., a book or sound recording).

Every effort has been made to ensure that the information in this manual is accurate. Polycom, Inc., is not responsible for printing or clerical errors. Information in this document is subject to change without notice.

About This Guide

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

Related Documentation

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

- *Polycom RealPresence Access Director Release Notes*
- *Polycom RealPresence Access Director Quick Start Guide*
- *Polycom RealPresence Access Director Getting Started Guide*
- *Polycom RealPresence Access Director Deployment Guide*

Required Skills

System administration of the RealPresence Access Director system requires planning and knowledge of Polycom video conferencing and video conferencing administration.

Polycom assumes the readers of this guide have a basic understanding of firewalls, SIP and H.323 signaling, media traversal, and networking concepts.

Contents

About This Guide	iii
Related Documentation	iii
Required Skills	iii
1 System Administration Overview	1
Logging into the System	1
Logging out of the System	2
Working with Administrator Accounts	2
Changing Your Password	3
Setting the Time Zone	3
Using the Dashboard	4
Working with Menus	5
Using Online Help	6
2 Configuration Summary	7
3 System Configuration	9
Setting the System Time	10
Configuring Network Settings	12
Using More than One Network Interface	15
Configuring Network Interface Settings	16
Editing Network Interface Settings	17
Working with Certificates	18
Accepted Forms of Certificates	19
How Certificates are Used	20
Certificate Procedures	20
Viewing Installed Certificates	21
Viewing Certificate Details	22
Adding a Certificate Authority's Public Certificate	23
Creating a Certificate Signing Request	24
Reviewing a Certificate	26
Adding a Signed Certificate	27
Replacing a Signed Certificate	28
Deleting Certificates	28
Provisioning the RealPresence Access Director System	29
Connecting to the Polycom Management System	30

	Disconnecting from the Polycom Management System	31
	Connecting to Microsoft Active Directory	31
	Mapping Roles to Active Directory Groups	32
	Working with Access Proxy Settings	33
	Configuring Access Proxy Settings	35
	Configuring SIP and H.323 Signaling Settings	36
	Editing SIP Settings	41
	Editing H.323 Settings	42
	Configuring Media Traversal Settings	43
	Editing Media Traversal Settings	44
	Configuring Federation Settings	45
4	User Management	47
	Adding a Local User Account	47
	Searching for a Local User Account	48
	Editing Local User Account Information	49
	Deleting a Local User Account	50
5	System Maintenance	51
	Managing Licenses	51
	Upgrading the Software	52
	Viewing Software Information	52
	Uploading an Upgrade Package File	53
	Installing an Uploaded Package File	53
	Upgrading in a Single Procedure	54
	Rolling Back to the Previous Software Version	54
	Shutting Down and Restarting the System	54
	Backing Up and Restoring	55
6	Troubleshooting	59
	Setting Custom Security for Network Access	59
	Using Active Call	60
	Working with System Log Files	60
	Downloading and Deleting Log Files	62
	Configuring Log Settings	63
	Running Dump Packet	66
	Running Ping	67
	Running Traceroute	67
	Troubleshooting Specific Issues	68

Remote Client Sign In Failed	69
Licensed Call Number is 0	71
SIP Registration Failed	71
SIP Call Failed	73
H.323 Call Failed	75
VMR Call Failed	77
No Audio, Video, or Content	77
Failed to Connect to RealPresence Resource Manager	78

System Administration Overview

The Polycom® RealPresence® Access Director™ system enables secure communication of high-quality video and audio between divisions or enterprises, remote users, and guest users. As a session border controller, the RealPresence Access Director system provides secure firewall traversal for all of the required connections.

As a system administrator of the RealPresence Access Director system, your role is to manage, monitor, and troubleshoot the day-to-day use of the system.

The following topics describe the initial steps for using the system:

- [Logging into the System](#)
- [Logging out of the System](#)
- [Working with Administrator Accounts](#)
- [Changing Your Password](#)
- [Setting the Time Zone](#)
- [Using the Dashboard](#)
- [Working with Menus](#)
- [Using Online Help](#)

Logging into the System

To log into the RealPresence Access Director system, you need:

- Microsoft® Internet Explorer® 8 or 9.
- Adobe® Flash® 9.0.124 or newer.

To log into the RealPresence Access Director system


- 1 Open a browser window and in the **Address** field enter the RealPresence Access Director system IP address:
 - **https://192.168.1.254:8443**
- 2 When the **Log In** screen appears, enter the following:
 - User ID: **admin**
 - Password: **admin**



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

Logging out of the System

To log out of the 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 your 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

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

- 3 Click **Associated Roles** and select **Administrator**.
- 4 Click  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 4-47 of this guide.

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.
- 5 Click **OK**.

Setting the Time Zone

After initial installation of the RealPresence Access Director system, the default time zone is Asia/Shanghai. After you launch the system for the first time, you must select the time zone of your geographic location.

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**.


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

- 4 Restart the system.

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 dashboard to display information that you want to see. The system saves your customization for subsequent logins.

To return to the dashboard from other functions, click .

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
 - Database
- **License Status.** This pane displays the number of:
 - Maximum Allowed Calls
 - Active SIP Calls
 - Active H.323 Calls

- **Peak Call Monitoring.** This pane displays the percentage of peak calls for:
 - H323
 - SIP



To add panes to the dashboard

- 1 Click **Add Panes**.
- 2 From the menu, select the panes that you want to display.

To close a pane

>> Click .

To resize a pane

- Click  to maximize.
- Click  to restore the default size.

To set the dashboard refresh rate

- 1 Click the arrow in the  Refresh: Every 15 seconds button.
- 2 Select an interval.

Working with Menus

When you log into the RealPresence Access Director system as an administrator, all of the system menus display, providing access to the functions necessary to monitor, maintain, and troubleshoot the system.

The table below lists each of the menus and their corresponding functions. The procedures for using each of the functions are described in the appropriate section of this Administrator's Guide.

User	Configuration	Maintenance
Users	Access Proxy Settings	License
	SIP and H.323 Settings	Software Upgrade
	Media Traversal Settings	Shutdown and Restart
	Federation Settings	Backup and Restore
Admin	Diagnostics	Help
Network Settings	Active Call	About RPAD
Time Settings	System Log Files	Help Contents
Certificates	Dump Packet	
Security Settings	Ping	
Log Settings	Traceroute	
Polycom Management System		
Microsoft Active Directory		

Using Online Help

To find help on a topic or function

- 1 In the **Contents** tab, click a topic to display the help.
- 2 In the **Index** tab, enter a keyword for the topic you need help on and press **Enter**.
- 3 In the **Search** tab, enter a word or words to search for and click **Go**. The help topics containing your words display.
 - Select **Highlight search results** to highlight your search term in each of the results.

Configuration Summary

This section lists the configuration and setup tasks required to complete your installation of the Polycom® RealPresence® Access Director™ system once the initial installation and network configuration are complete.

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

The table below shows the recommended order for completing configuration and setup of the RealPresence Access Director system. For detailed instructions, refer to the specific sections listed in the table and included in this document.

To	Refer To
Set the system time zone	“Setting the System Time” on page 3-10
Configure the network interface settings	“Configuring Network Settings” on page 3-12
Manage the system certificates	“Working with Certificates” on page 3-18
Connect to the Polycom management system	“Connecting to the Polycom Management System” on page 3-30
Connect to Microsoft Active Directory	“Connecting to Microsoft Active Directory” on page 3-31
Configure the Access Proxy settings	“Working with Access Proxy Settings” on page 3-33
Configure the SIP and H.323 signaling settings	“Configuring SIP and H.323 Signaling Settings” on page 3-36
Configure the media traversal settings	“Configuring Media Traversal Settings” on page 3-43
Configure the federation settings	“Configuring Federation Settings” on page 3-45

System Configuration

After the Polycom® RealPresence® Access Director™ system has been installed and configured with initial settings, you can configure additional network and communication settings for your system.

For information on initial installation and network configuration procedures, see the *RealPresence Access Director Getting Started Guide* (available at support.polycom.com).

The following topics discuss configuration of the RealPresence Access Director system:

- [Setting the System Time](#)
- [Configuring Network Settings](#)
- [Working with Certificates](#)
- [Connecting to the Polycom Management System](#)
- [Connecting to Microsoft Active Directory](#)
- [Working with Access Proxy Settings](#)
- [Configuring SIP and H.323 Signaling Settings](#)
- [Configuring Media Traversal Settings](#)
- [Configuring Federation Settings](#)

Setting the System 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.

The **Time Settings** function in the RealPresence Access Director system allows you to edit time settings when necessary. Consider the following before changing the time settings.

- The RealPresence Access Director system displays two different time settings:
 - 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: The system displays the server time in the **Server Time (Refresh every 10 seconds)** field. 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.
- Changing the time settings requires a system restart, which terminates active calls and logs all users out of the system.
- If your system uses a CA-provided identity certificate, changing the system time zone may invalidate the certificate. If this happens, you must request and install a new certificate.
- Changing the time settings can affect the number of days available for a trial period license.

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	<p>The time zone in which your RealPresence Access Director system is located.</p> <p>Notes</p> <ul style="list-style-type: none"> • 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. • 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.
Auto adjust for Daylight Saving Time	<p>Automatically determined in accordance with the system time zone. If the system time zone you select observes Daylight Saving Time, this setting is enabled.</p> <p>Note</p> <p>The administrator cannot change this setting.</p>
Manually set system time	<p>Note</p> <p>Polycom strongly recommends that you do not set the time and date manually.</p>

Field	Description
NTP servers	<p>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.</p> <p>See the <i>Polycom RealPresence Access Director Deployment Guide</i> for additional information about NTP servers</p> <p>Note</p> <p>Polycom recommends that you specify at least two NTP servers for maintaining system time.</p>

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.

Configuring Network Settings

During system installation, most network settings are specified for one network interface (eth0). In this initial configuration, all management, signaling, external media, and internal media communications are bonded only to the eth0 network interface.

The RealPresence Access Director system includes four network interface cards (NICs). You can configure the management, signaling, external media, and internal media communication services based on the number of network cards you use.

In addition to four physical network interfaces, the RealPresence Access Director system enables administrators to bind multiple network interfaces together into a single channel and a special network interface called a channel bonding interface. Channel bonding enables two or more network interfaces to act as one, which increases the available bandwidth and provides redundancy. Each channel bonding interface appears as a single network interface to applications that access it.



The channel bonding functionality is not available in this release of the RealPresence Access Director system.

The following table describes the RealPresence Access Director system network settings. After initial installation of the system, most of the default values represent one network interface (eth0).

Element	Description	Default Value
General Network Settings		
Hostname	Hostname of the RealPresence Access Director system. Hostname may contain only letters, numbers, and internal hyphens. The reserved values appserv* and dmamgk-* cannot be used for host names.	Installation default
Primary DNS	IP address of the primary Domain Name Server (DNS) for the network to which the system connects.	Installation default
Secondary DNS	IP address of the secondary DNS server for the network to which the system connects.	
Tertiary DNS	IP address of the tertiary DNS server for the network to which the system connects.	
Search Domain	One or more domain names, separated by spaces. The system domain from the Domain field is added automatically.	
Domain	Domain of the RealPresence Access Director system. <Host Name> . <Domain>	

Element	Description	Default Value
Advance Network Settings		
Interface	Name of the network interface.	Installation default for eth0, eth1, eth2, eth3
Device	MAC address and name of the network card.	Installation default for eth0, eth1, eth2, eth3
IPv4 Address	IPv4 address of the access server interface.	Installation default for eth0
IPv4 Subnet Mask	Subnet mask of the IP address. This field accepts only IPv4 format input.	Installation default for eth0
IPv4 Default Gateway	IPv4 address of the default gateway.	Installation default for eth0
Service Network Settings		
Network interface of signaling	IP address of the network interface that handles SIP and H.323 signaling and Access Proxy traffic.	Installation default for eth0
External Relay IP	IP address of the network interface that handles media relay between the RealPresence Access Director system and external networks.	Installation default for eth0
Internal Relay IP	IP address of the network interface that handles media relay between the RealPresence Access Director system and the internal enterprise network.	Installation default for eth0
Management IP	IP address of the network interface that handles management traffic, including the web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.	Installation default for eth0
Deployed behind Outside Firewall	<p>Enable this setting in the following situations:</p> <ul style="list-style-type: none"> If the system is deployed behind an outside firewall/NAT (enables 1:1 NAT mapping address in the outside firewall). If the system is deployed in the trust (LAN) side. <p>Disable if the system is deployed behind an outside firewall without NAT.</p>	Disabled

Element	Description	Default Value
Signaling Relay Address	<p>Specifies the signaling address for remote clients. This address must be the public IP address of the RealPresence Access Director system mapped on a firewall.</p> <p>Note</p> <p>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 Address instead of FQDN to establish a TLS connection to the system.</p>	None
Media Relay Address	<p>Specifies the media address for remote clients. This address must be the public IP address mapped on a firewall.</p>	None

Using More than One Network Interface

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.

You can bundle the management, signaling, external media, and internal media communication services on one or three network adapters, or separate each service by using all four network interfaces.

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

Number of Configured Network Interfaces	eth0	eth1	eth2	eth3
1	<ul style="list-style-type: none"> • Management • SIP and H.323 signaling • External media • Internal media 			
3	<ul style="list-style-type: none"> • Management • SIP and H.323 signaling 	<ul style="list-style-type: none"> • External media 	<ul style="list-style-type: none"> • Internal media 	
4	<ul style="list-style-type: none"> • Management 	<ul style="list-style-type: none"> • SIP and H.323 signaling 	<ul style="list-style-type: none"> • External media 	<ul style="list-style-type: none"> • Internal media

Configuring Network Interface Settings



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.

To configure more than one network interface

- 1 Go to **Admin > Network Settings > General network setting**.
- 2 Complete the general settings for the network interface as needed. Entry fields marked with an asterisk (*) are required.
- 3 Click **Advance network setting > Configuration Wizard**.
- 4 In the **Step 1 of 3: Eth Bond** dialog box, click **Next**.
The channel bonding functionality is not available in this release of the RealPresence Access Director system.
- 5 In the **Step 2 of 3: Advance Network Settings** dialog box, click the network interface to configure and complete the required fields.

- 6 Click **Next**.
- 7 In the **Step 3 of 3: Service Network Settings** dialog box, select the IP address for the following fields:
 - Network interface of signaling
 - External Relay IP
 - Internal Relay IP
 - Management IP
- 8 Select **Deployed behind Outside Firewall** if the RealPresence Access Director system is deployed behind the enterprise's outside firewall/NAT.
 - If selected, enter the **Signaling relay address** and **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 Address instead of FQDN to establish a TLS connection to the RealPresence Access Director system.

- 9 Click **Done > Commit** and **Reboot Now** to save the network settings.
- 10 After the system restarts, repeat the steps above to configure additional network interface cards as needed.

Editing Network Interface Settings

You can edit the network settings for each interface when necessary.



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 the signaling relay address.

To edit network settings

- 1 Go to **Admin > Network Settings**.
The **General network setting** tab displays.
- 2 Revise the general network settings as needed. Entry fields marked with an asterisk (*) are required.
- 3 Choose one of the following actions:

- If you are done editing, click **Update** to save the changes and restart the system.
 - To edit both advanced network settings and service network settings click the **Advance Network Setting** tab and complete the steps below.
- 4** Click **Configuration Wizard**.
 - 5** In the **Step 1 of 3: Eth Bond** dialog box, click **Next**.

The channel bonding functionality is not available in this release of the RealPresence Access Director system.
 - 6** In the **Step 2 of 3: Advance Network Settings** dialog box, click the network interface to revise and edit the settings as needed.
 - 7** Click **Next**.
 - 8** Revise the service network settings as needed.
 - 9** Click **Done > Commit** and **Reboot Now** to save your revisions and restart the system.

To edit only the service network settings

- 1** Click **Admin > Network Settings > Service Network setting**.
- 2** Revise the service network information as needed.
- 3** Click **Update** to save the changes and restart the system.



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 Address instead of FQDN to establish a TLS connection to the RealPresence Access Director system.

Working with Certificates

X.509 certificates are a security technology that assists networked computers in determining whether to trust each other.

- A single, centralized certificate authority (CA) is established. Typically, this is either an enterprise's IT department or a commercial certificate authority.
- Each computer on the network is configured to trust the central certificate authority.
- Each server on the network has a public certificate that identifies 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.

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: <ul style="list-style-type: none"> • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Intermediate certificates (optional). <p>Note Upload the file or paste into text box.</p>
	CER (single certificate) file	A signed certificate for the system, authenticating its public key. <p>Note Upload file or paste into text box.</p>
DER (binary format using ASN.1 Distinguished Encoding Rules)	PKCS #7 protocol P7B file	A certificate chain containing: <ul style="list-style-type: none"> • A signed certificate for the system, authenticating its public key. • The CA's public certificate. • Intermediate certificates (optional). <p>Note Upload the file.</p>
	CER (single certificate) file	A signed certificate for the system, authenticating its public key. <p>Note Upload the file.</p>

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 management interface, the RealPresence Access Director system (server) 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 server offers an X.509 certificate to identify itself.
- When a client sends SIP messages with TLS transport, the RealPresence Access Director system server 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 Polycom Distributed Media Application™ (DMA™) systems, and install the CA certificates on each client.

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 a public certificate signed by your certificate authority that identifies the RealPresence Access Director system.
- Remove a signed certificate or a certificate authority's certificate.

Viewing Installed Certificates

To view installed certificates

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

The table below describes the certificate information that displays.

Field	Description
Enable OCSP	<p>Enables the use of Online Certificate Status Protocol to obtain the revocation status of a certificate presented to the system.</p> <p>When enabled, the system checks the certificate's AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder:</p> <ul style="list-style-type: none"> • 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	<p>KEY_STORE contains the signed certificate that identifies the RealPresence Access Director system.</p> <p>TRUSTED_STORE contains trusted certificates, such as CA certificates.</p>
Purpose	<p>The purpose of the certificate for the RealPresence Access Director system.</p> <ul style="list-style-type: none"> • 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.
Expiration	The expiration date of the certificate.

To Use 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.

Viewing Certificate Details

To view detailed information about certificates

- 1** Go to **Admin > Certificates**.
- 2** Select the certificate to view.
- 3** Click **Display Details**.

Certificate Details displays the following information:

Section	Description
Purpose	<p>The purpose of the certificate for the RealPresence Access Director system.</p> <ul style="list-style-type: none"> • 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.
Issued To	
Common Name (CN)	<p>For a Server SSL certificate, the fully qualified domain name (FQDN) of the system's management interface, as defined by the host name and domain that are specified in Admin > Network Settings.</p> <p>For a CA certificate, the common name of that certificate.</p>

Section	Description
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	
Issue date	The date the certificate was issued.
Expiration 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.

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 thus 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.

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 See Admin > Network Settings .
Domain	Optional.

Field	Description
Organizational unit (OU)	Optional. The subdivision of your organization, such as Human Resources or IT, that is handling the certificate.
Organization (O)	Optional. Usually, the legal name of your enterprise.
City or locality (L)	Optional.
State (ST)	Optional.
Country (C)	Required. 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 email 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 email text, email 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

>> 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.

CAUTION



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.

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 3-24.
- 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 3-27
- 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 RealPresence Access Director System

The RealPresence Access Director system can have some of its configuration settings provisioned by the Polycom RealPresence Resource Manager system. Alternately, you can configure all system settings manually.

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.
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.

Field	Description
Directory Server (LDAP Server)	The IP address of the internal LDAP server that the system forwards to when endpoints behind the system try to connect to the LDAP server.
Verify Certificate (LDAP Server)	Configures whether a certificate needs to be verified between the RealPresence Access Director system and the LDAP server.
Presence Server (XMPP Server)	The IP address of the internal presence server that the system forwards to when endpoints behind the system try to connect to the presence server.
Verify Certificate (XMPP Server)	Configures whether a certificate needs to be verified between the RealPresence Access Director system and the presence server.

Connecting to the Polycom Management System

To enable provisioning, the RealPresence Access Director system must connect to the RealPresence Resource Manager system.

For information about configuring the RealPresence Resource Manager system to provision the RealPresence Access Director system, refer to the *Polycom RealPresence Access Director Deployment Guide*.

To connect to the RealPresence Resource Manager system for provisioning

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

Field	Description
Login Name	The name of the RealPresence Access Director system administrator
Password	The password of the RealPresence Access Director system administrator
Address	The IP address of the RealPresence Resource Manager system

Field	Description
Verify certificate from internal server	<p>Enable if certificates need to be verified between the RealPresence Access Director system and the RealPresence Resource Manager system.</p> <p>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.</p>

3 Click **Connect**.

The RealPresence Resource Manager system provisions some of the settings for the RealPresence Access Director system. The administrator supplies additional configuration details as described in this chapter.

Disconnecting from the Polycom Management System

To disconnect from the RealPresence Resource Manager System

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

Connecting to Microsoft Active Directory

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

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

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 IP address	The IP address of the Active Directory server.
Domain\User name	The domain and user name that the RealPresence Access Director system uses to log in to Active Directory and retrieve domain and group information.
Password	The password that the RealPresence Access Director system uses to log in to 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=Po1ycom,DC=com The RealPresence Access Director system fetches Active Directory domains from the specified base DN.

4 Click **Update**.

Mapping Roles to Active Directory Groups

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.
 - **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 RealPresence Access Director system uses Access Proxy to enable remote clients to be provisioned and managed by the Polycom RealPresence Resource Manager system. When Access Proxy receives an HTTPS, LDAP, or XMPP request from an external endpoint, the RealPresence Access Director system accepts the request for resources and forwards it to the internal HTTPS, LDAP, or XMPP server specified in the RealPresence Resource Manager system.

Access Proxy settings are configured manually by the RealPresence Access Director system administrator or through provisioning by the RealPresence Resource Manager system.

When the RealPresence Access Director system is provisioned, the RealPresence Resource Manager system provides the settings listed below for the LDAP, and XMPP protocols.

- Next hop address
- Next hop port
- Verify certificate from internal server

For the HTTPS protocol, the RealPresence Access Director system configures the settings listed above after it is provisioned by the RealPresence Resource Manager system.

To display the current Access Proxy settings

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

The table of current settings is displayed. After a new installation, default values are shown for settings except **Next hop address**, which is blank.

Setting	Description
Protocol	HTTPS, LDAP, or XMPP
External IP External listening port	<p>The external IP address of the Access Proxy server, used by the remote client to connect to the RealPresence Access Director system.</p> <p>The ports at which the Access Proxy server listens.</p> <p>By default, the ports are as follows:</p> <ul style="list-style-type: none"> • For HTTPS: 443 • For LDAP: 389 • For XMPP: 5222 <p>Note The External listening port field displays only when you edit Access Proxy settings.</p>
Require client certificate from the remote endpoint	<p>When selected, Access Proxy requests and verifies the client certificate.</p> <p>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.</p>
Internal IP	The internal IP address of Access Proxy. Access Proxy connects to the RealPresence Resource Manager system at this address.

Setting	Description
Next hop address	<p>The IP address of the internal server (the RealPresence Resource Manager system).</p> <p>Note This value is blank after a new installation.</p>
Next hop port	<p>The port at which the RealPresence Resource Manager system listens.</p> <p>The default ports are:</p> <ul style="list-style-type: none"> • HTTPS: 443 • LDAP: 389 • XMPP: 5222 <p>Note The Next hop port field displays only when you edit Access Proxy settings.</p>
Verify certificate from internal server	<p>When selected, Access Proxy verifies the certificate from the internal server (the RealPresence Resource Manager system).</p> <p>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.</p>

Configuring Access Proxy Settings

To manually configure Access Proxy settings

- 1 Go to **Configuration > Access Proxy Settings**.
- 2 Select **HTTPS, LDAP, or XMPP**.
- 3 Under **Actions**, click **Edit**.
- 4 For **Next hop address**, verify or enter the IP address of the RealPresence Resource Manager system.

- 5 Enter the following **Next hop port** values:
 - HTTPS: 443
 - LDAP: 389
 - XMPP: 5222
- 6 Enter or verify the values for the other settings.
- 7 Click **OK** to save the configuration.
- 8 In the **Confirm Action** dialog box, click **Yes** to restart Access Proxy.

To edit HTTPS Access Proxy settings after provisioning

- 1 Connect to the RealPresence Resource Manager system.
For detailed information, refer to [“Connecting to the Polycom Management System”](#) on page 3-30.
- 2 Go to **Configuration > Access Proxy Settings**.
- 3 Select **HTTPS**.
- 4 Under **Actions**, click **Edit**.
- 5 For **Next hop address**, verify or enter the RealPresence Resource Manager IP address.
- 6 For **Next hop port**, enter 443.
- 7 Click **OK** to save the configuration.
- 8 In the **Confirm Action** dialog box, click **Yes** to restart Access Proxy.

Configuring SIP and H.323 Signaling Settings

The table below describes the settings to configure for SIP signaling and H.323 signaling. An asterisk (*) indicates a required field. For more information, refer to the *Polycom RealPresence Access Director Deployment Guide*.

Field	Description
SIP Settings	
Enable SIP signaling	<p>When selected, enables the system to operate as a SIP server, transmitting SIP requests and responses for SIP devices.</p> <p>Caution Disabling SIP terminates any existing SIP calls.</p>

Field	Description
External Port Settings	
Port name	Specifies the purpose of the external port, for example, encrypted or unencrypted.
Port number	The number of the external port. 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.
Transport	The transport protocol of the port.
Require certificate	Specifies whether a certificate is required from the remote endpoint.
Dial string policy	Enable if the RealPresence Access Director system uses the dial string of a DMA system to route calls from this port.
Prefix of Userinfo	The prefix that the RealPresence Access Director system adds to the request line of the SIP invite message. Note This prefix must also be defined in the 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 DMA system. If not defined, the DMA system will reject calls.
Forbid registration	When selected, prohibits SIP registration for the port.

Field	Description
Internal Port Settings	
Unencrypted SIP port	<p>The protocol the system uses for unencrypted SIP connections and the associated listening port number.</p> <p>Default UDP/TCP port is 5070.</p> <p>Note</p> <p>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.</p>
TLS port	<p>The listening TLS port number the system uses for encrypted SIP connections.</p> <p>Default TLS port number is 5071.</p> <p>Note</p> <p>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.</p> <p>If SIP signaling is enabled, TLS is automatically supported.</p>
SIP registrar (Next hop) address	<p>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.</p> <p>The port number of the SIP registrar server must be the same as the port on which the SIP server in the DMA system listens. The transport protocol must be supported by the SIP registrar server. UDP is the default transport protocol.</p> <p>Note</p> <p>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.</p> <p>When AUTO is selected, the transport protocol depends on the DNS query result for the SIP registrar address.</p> <p>Only TCP and TLS are available for transport when TCP is selected for the unencrypted SIP port.</p>

Field	Description
SIP proxy (Next hop) address	<p>The IP address or FQDN of the SIP proxy server, and the destination port number and transport protocol the system uses to communicate with the SIP proxy server.</p> <p>The port number of the SIP proxy server must be the same as the port on which the SIP server in the DMA system listens. The transport protocol must be supported by the SIP proxy server. UDP is the default transport protocol.</p> <p>Note</p> <p>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.</p> <p>When AUTO is selected for transport, the transport protocol depends on the DNS query result for SIP proxy address.</p> <p>Only TCP and TLS are available for transport when TCP is selected in unencrypted SIP port.</p>
Registration refresh interval	<p>Specifies how often registered SIP endpoints send keep-alive messages to the SIP registrar server.</p> <p>Must be greater than or equal to the minimum SIP registration interval that the SIP registrar server allows.</p> <p>Range is 1–99999.</p> <p>Default value is 300.</p>
RFC5626 keep-alive interval	<p>The Flow-Timer value for an RFC5626 endpoint.</p> <p>Range is 1-99999.</p> <p>Default value is 120.</p>
H.323 Settings	
Enable H.323 signaling	<p>Enables the system to operate as an H.323 server, transmitting H.323 requests and responses for H.323 devices.</p> <p>Caution</p> <p>Disabling H.323 terminates any existing H.323 calls.</p>

Field	Description
H.225 RAS port	<p>The listening port number the system uses for LRQ messages.</p> <p>Default value is 1719.</p> <p>Note</p> <p>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.</p>
H.225 call signaling port	<p>The listening port number the system uses for Q.931 messages.</p> <p>Default value is 1720.</p> <p>Note</p> <p>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.</p>
Gatekeeper (Next hop) address	The IP address or FQDN of the H.323 gatekeeper.
RAS port (Gatekeeper)	<p>The listening port number of the gatekeeper.</p> <p>Note</p> <p>Polycom recommends that you use the default port range 0-65535.</p>
H.225 call signaling port (Gatekeeper)	<p>Note</p> <p>Polycom recommends that you use the default port range 0-65535</p>
CIDR	<p>Classless Inter-Domain Routing. Distinguishes the internal network and the external network when the system is behind the enterprise's firewall/NAT. The system considers the IP addresses in CIDR to be addresses within the enterprise network.</p> <p>The value of CIDR depends on the mode of the local DMA system.</p> <ul style="list-style-type: none"> • If the local DMA system is in Routed mode, the CIDR should include only the IP address of the DMA system. • If the local DMA system is in Direct mode, the CIDR should include the subnet of the DMA system and local enterprise endpoints.

Editing SIP Settings

To edit the SIP settings

- 1 Go to **Configuration > SIP and H.323 Settings**.
- 2 In **SIP Settings**, revise the fields as needed.
- 3 Under **Actions**, click **Update** to refresh the fields.

To add an external SIP port

- 1 Go to **Configuration > SIP and H.323 Settings**.
- 2 Click **Add** next to the **External Port Settings** list.
- 3 Complete the following fields:

Field	Description
Port number	The number of the external port. 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 name of the external port for the remote user or enterprise.
Dial string policy	Select if you are using a dial string to route incoming call requests.
Prefix of Userinfo	If Dial string policy is enabled, specifies the prefix to add to the request line of the SIP invite message.
Host	If Dial string policy is enabled, specifies the host name or FQDN of the port.
Forbid registration	When selected, prohibits SIP registration for the port.

- 4 Click **OK**.
- 5 Click **Update**.

To delete an external SIP port

- 1 Go to **Configuration > SIP and H.323 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.

To edit an external SIP port

- 1 Go to **Configuration > SIP and H.323 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**.

Editing H.323 Settings

To edit the H.323 settings

- 1 Go to **Configuration > SIP and H.323 Settings**.
- 2 In **H.323 Settings**, revise the fields as needed.
- 3 Under **Actions**, click **Update** to refresh the fields.

To add a CIDR IP address

- 1 Go to **Configuration > SIP and H.323 Settings**.
- 2 In **H.323 Settings > CIDR**, enter the CIDR as follows:
 - If the local DMA system is in Routed mode, enter the IP address of the DMA system.
 - If the local DMA system is in Direct mode, enter the subnet of the DMA system and local enterprise endpoints.

- 3 Click **Add**.

The subnet displays below the **CIDR** field.

- 4 In **CIDR**, enter the H.323 gatekeeper address in the subnet of the DMA system.
- 5 Click **Add**.

The H.323 gatekeeper subnet displays below the **CIDR** field.

To delete a CIDR IP address

- 1 Go to **Configuration > SIP and H.323 Settings**.
- 2 In **H.323 Settings**, below the **CIDR** field, select the CIDR IP address to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

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.

The table below describes the settings to configure for media traversal connections. For more information, refer to the *Polycom RealPresence Access Director Deployment Guide*.

Field	Description
Media Relay	
External Relay IP Address	The media relay IP address for remote and external users.
Internal Relay IP Address	The media relay IP address for internal users.
Band Width Limitation	The call bandwidth limitation in Mbps.
Enable QOS	Enable Quality of Service in the media packets relayed by the system.
QOS Setting	<p>Specifies 11 types of Diffserv and enables you to choose how to set the priority of media packets relayed by the system for video, audio, and far-end camera control.</p> <p>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.</p>

Field	Description
Neighbor RPAD Media Addresses	<p>If there are multiple RealPresence Access Director systems behind the outside firewall, add the internal media IP addresses of those devices.</p> <p>For example:</p> <ul style="list-style-type: none"> • Two RealPresence Access Director systems are located behind the outside firewall. • Two SIP remote users register separately to the SIP registrar server through these two systems. • A SIP call is established between these two SIP remote users. <p>The internal media address of each RealPresence Access Director system must be configured on both RealPresence Access Director systems.</p>

Editing Media Traversal Settings

To edit the media traversal settings

- 1 Go to **Configuration > Media Traversal Settings**.
- 2 Revise the settings as needed.
- 3 Under **Actions**, click **Update** to refresh the fields.

To add a neighboring RPAD media address

- 1 Go to **Configuration > Media Traversal Settings**.
- 2 In **Neighbor RPAD Media Addresses**, enter the internal media IP address of the neighbor RealPresence Access Director system.
- 3 Click **Add**.

To delete a neighboring RPAD media address

- 1 Go to **Configuration > Media Traversal Settings**.
- 2 Under the **Neighbor RPAD Media Addresses** field, select the neighbor RealPresence Access Director system to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

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 the *Polycom RealPresence Access Director Deployment Guide*.

To view 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).

To search for a federation

- 1 Go to **Configuration > Federation Settings**.
- 2 Complete the **Type**, **Status**, and **Company Name** fields as needed and click **Search**.

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
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**.

User Management

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

The RealPresence Access Director system provides user roles, each with its own set of privileges, to facilitate management of the system. When creating a local user account, you can assign one or more user roles to each user.

This section describes the following user management options:

- [Adding a Local User Account](#)
- [Searching for a Local User Account](#)
- [Editing Local User Account Information](#)
- [Deleting a Local User Account](#)

Adding a Local User Account

The table below describes the user roles available in the RealPresence Access Director system:


Role	Description
Administrator	Performs system configuration, management, and ongoing system administration. The administrator has full privileges to operate the system.
Auditor	Views active calls, manages system log files, and uses dump package, ping, and traceroute to diagnose system issues.
Provisioner	Performs a subset of administrator responsibilities, such as partial configuration and services. The provisioner role is intended to facilitate daily activities, such as personnel changes and troubleshooting call problems, for large deployments. However, these activities do not require privileges such as system reconfiguration.

Only administrators can add user accounts.

To add a local user 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
Password	User's system login password
Confirm Password	Repeat user's system login password

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

- 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 Do one of the following:
 - Enter a string in one or more of the search fields:
 - » Search users
 - » User ID
 - » First name
 - » Last name
 - Click the arrow in the **Role** field, and select a user role.
- 4 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.

Editing Local User Account Information

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

To edit user information

- 1 Go to **User > Users**.
- 2 Select a user account from the list.
- 3 Click **Edit**.
- 4 Enter the updated identification and user role information.
- 5 Click **OK**.

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**.

Deleting a Local User Account

Only Administrators can delete user accounts.



Be aware of the following before deleting a user account:

- When you delete an account, all 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; therefore, the last local Administrator account cannot be deleted.
- Administrators cannot delete their own accounts.

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 Polycom® RealPresence® Access Director™ system provides maintenance functions to ensure consistent, high-quality system performance:

- [Managing Licenses](#)
- [Upgrading the Software](#)
- [Shutting Down and Restarting the System](#)
- [Backing Up and Restoring](#)

Managing Licenses

The RealPresence Access Director system is licensed for the number of concurrent calls it can manage. A trial period license for five calls is included with each new RealPresence Access Director system.

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.
Trial period	The time remaining in the trial period. Commercial licenses have no trial period limitation.

Field	Description
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 redeemed the license number.

To activate a license

- 1 Go to **Maintenance > License**.
- 2 Enter the **Activation key** for the license and click **Update**.

Upgrading the Software

The RealPresence Access Director system's upgrade functionality includes the capability of rolling back to the previous version. Only Administrators can upgrade or roll back system software versions.

The system enables you to upload a package file from the local system for later installation, and to upload and install a package file in one operation.



Use caution when upgrading or rolling back to a previous system version. Upgrading and rolling back require a system restart, which terminates active calls and logs all users out of the system. Polycom recommends that you download necessary backup files before beginning an upgrade.

Viewing Software Information

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

- Click **Help > About RPAD**.
- For more detailed information, go to **Maintenance > Software Upgrade**.

In addition to the current software version, the **Software Upgrade** page displays, if applicable:

- Upgrade and roll back versions
- History of upgrade actions that have been performed

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 advises 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.

To upload a package file for later installation

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

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

- 4 Click **Close**.

The **Upgrade Package Details** section of the **Software Upgrade** page displays information about the file that you uploaded.

Installing an Uploaded Package File

The upgrade installation procedure automatically creates a backup file, which you can use to roll back to the current 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.

If an upgrade package has been uploaded, the **Actions** menu displays the **Upgrade** option.



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 Verify that the uploaded package file is the one that you want to install.
- 4 In the **Confirm Action** dialog box, click **Yes**.

The system notifies you that the upgrade is starting.

- 5 Click **OK** to log out.

Upgrading in a Single Procedure

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.

Rolling Back to the Previous Software Version

If a downgrade package file is available, the **Actions** menu displays the **Roll Back** option, and the **Software Upgrade** page displays information about the roll back version.

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 might be lost.

To roll back the system to the previous version

- 1 Go to **Maintenance > Software Upgrade**.
- 2 Under **Version Information**, verify that the roll back version described 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.

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**.

Active calls are terminated, active users are logged out, and the server remains powered off until manually powered on.

To restart (reboot) the system

- 1 Go to **Maintenance > Shutdown and Restart**.
- 2 Click **Restart**.
- 3 In the **Confirm Action** dialog box, click **Yes**.

Active calls are terminated and active 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, host name, 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. Generated automatically by the system 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 download a backup file to a local machine

- 1 Go to **Maintenance > Backup and Restore**.
- 2 Select the backup file to download.
- 3 Under **Actions**, click **Download Selected**.
- 4 Choose the location on the local machine to save the file and click **Save**.

The progress of the file download displays. Click **Close** when the download is complete.

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. 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 you will 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 the 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.

Troubleshooting

The Polycom® RealPresence® Access Director™ system provides diagnostic and troubleshooting tools to ensure optimum performance of the system.

The following administrator functions assist in troubleshooting system performance:

- [Setting Custom Security for Network Access](#)
- [Using Active Call](#)
- [Working with System Log Files](#)
- [Configuring Log Settings](#)
- [Running Dump Packet](#)
- [Running Ping](#)
- [Running Traceroute](#)
- [Troubleshooting Specific Issues](#)

Setting Custom Security for Network Access

Custom security mode enables the following secure network access methods:

- Linux Secure SHell access
- Access Proxy white list authentication for LDAP and XMPP access

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 **Allow Linux SSH access**.
- 3 Select or deselect **Enable Access Proxy white list authentication for LDAP and XMPP access**.

- 4 Click **Update**.
- 5 Click **Yes** to confirm your selections.

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.

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](#).

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 active bandwidth, adjusted bandwidth, bandwidth limitation, and number of licensed calls.
activeCallAuditor	Active call monitoring information, including peak call data.
utility	Information on all system utility modules, such as scheduling and date utilities.
sipService	Information on SIP calls, such as caller, endpoint recipient, contact, user agent, max forwards, expiration, route, path, and content length.
h323Service	Information about H.323 calls and the behavior of the relative components, such as handling H.323 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 6-63.
mediaTraversal	Information on a call's media session, such as start, stop or restart. Also logs the media path information as a route entry. Contains 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.

Name	Contents of Log
accessProxy	Information about an endpoint's message exchanges with the internal server. Message exchanges include login, contact searches, and presence status. Logged information about message exchanges includes message source IP address and port, message destination IP address and port, message protocol, and message content details (if the logging level is DEBUG). See "Configuring Log Settings" on page 6-63 for details on setting the logging level.
serviceController	Information on the service controller module, which controls other system components.

Downloading and Deleting 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	Host name of the RealPresence Access Director system server.
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.
Type	Indicates whether the log is active or archived.

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 From the **Actions** menu, select **Download Logs**.
- 5 In the **Save As** dialog box, select a location, and choose **Save**.

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 From the **Actions** menu, select **Delete Logs**.
- 5 In the **Confirm Action** dialog box, Click **Yes** to delete the log file.

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 files 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.	Daily

Field	Description	Default Value
Retention period (days)	The number of days that the system retains archived log files before deleting them. 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 maximum size of the log file. Range: 1 MB - 100 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. 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
Source log files	The source log files that syslog-ng uses to retrieve logs that will be forwarded to the remote server.	All

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	Fine-grained information that is useful for debugging the system.
Info	Normal operational messages that highlight the progress of the system and do not require any action.
Warn	Warning messages that indicate an error will occur if action is not taken. Warn is the default logging level.
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.
- 3 To configure the settings for a remote syslog server, click **Add**.
 - 4 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 IP	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.

Field	Description
Severity filter	<p>The event severity filter to apply to the remote syslog server.</p> <p>Default value is Debug.</p> <p>Options</p> <ul style="list-style-type: none"> Debug Info Notice Warning Err Crit Alert Emerg

- 5 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
 - WEBADMIN
- 6 Click  to add the source files to the **Selected source files** list.
- 7 Click **OK** to add the remote syslog server settings.
- 8 Click **Update** to process all changes to the log settings.

Running Dump Packet

Use Dump Packet to create a file containing information about the content of packets crossing the network.

To run Dump Packet

- 1 Go to **Diagnostics > Dump Packet**.
- 2 Select the packet data to capture.

- 3 Select **All (including media packet)** to capture SIP, H.323, Access Proxy, and media packets.
- 4 Click **Dump** to start the packet data capture.
- 5 Click **Stop** to stop the capture.

The RealPresence Access Director system generates a .pcap dump file and creates a prompt in **Diagnostics > System Log Files** to retrieve the dump file.

Running Ping

Use **Ping** to verify that the server can communicate with another node on the network.

To run Ping on each server

- 1 Go to **Diagnostics > Ping**.
- 2 Enter an IP address or host name.
- 3 Click **Ping** to display the results of the command.

Running Traceroute

Use **Traceroute** to view the route that the server uses to reach a specified address and the latency (round trip) for each hop.

To run Traceroute on each server

- 1 Go to **Diagnostics > Traceroute**.
- 2 Enter an IP address or host name.
- 3 Click **Trace** to display the results of the command.

Troubleshooting Specific Issues

Refer to the sections below for the recommended troubleshooting actions for specific issues.

- [Remote Client Sign In Failed](#)
- [Licensed Call Number is 0](#)
- [SIP Registration Failed](#)
- [SIP Call Failed](#)
- [H.323 Call Failed](#)
- [VMR Call Failed](#)
- [No Audio, Video, or Content](#)
- [Failed to Connect to RealPresence Resource Manager](#)

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
<p>Access Proxy error</p>	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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: <p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to Admin > Troubleshooting Utilities > Test Network > Ping. • Check whether the RealPresence Access Director system is accessible. <p>On the inside firewall</p> <ul style="list-style-type: none"> • Check the firewall policy to determine if the HTTPS, LDAP, and XMPP ports all permit calls from untrust to trust zone. Default values are: <ul style="list-style-type: none"> – HTTPS: TCP 443 – LDAP: TCP 389 – MPP: TCP 5222 <p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • Wait 10 minutes, then check whether Access Proxy is running. • Restart the system if Access Proxy is still not running.
<p>Firewall configuration error</p>	<p>On the outside firewall</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – HTTPS: TCP 443 – LDAP: TCP 389 – XMPP: TCP 5222

Possible Reasons	Recommended Actions
Certificate check fails	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to Admin > Topology > Sites. • Check whether the signaling IP address of the RealPresence Access Director system is included in the subnets.
User configuration error	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • 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	<p>Purchase a license.</p> <p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> Go to Maintenance > License > Activation key and enter the new key. Click Update.
License is invalid due to system time being changed.	<p>If you have purchased a license, in the RealPresence Access Director system</p> <ul style="list-style-type: none"> Go to Maintenance > License > Activation key and re-enter the license activation key. Click Update. <p>If you have a trial license, you must re-install the RealPresence Access Director system server to generate a new trial period license.</p> <p>CAUTION</p> <p>If you reinstall the system server, all manually configured or provisioned settings will be lost.</p>

SIP Registration Failed

Possible Reasons	Recommend Actions
SIP component not running	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> 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	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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. <p>In the DMA system</p> <ul style="list-style-type: none"> • 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	<p>On the remote client</p> <ul style="list-style-type: none"> • Check whether the SIP registrar server address is the public address of the RealPresence Access Director system.
TLS port error	<p>In the RealPresence Access Director system</p> <p>When TLS is selected as the transport protocol between the RealPresence Access Director system and the DMA system, ensure that the port is 5061, not 5060..</p>
Site configuration error	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to Admin > Topology > Sites. • Check whether the SIP registrar server address for remote clients is the public address of the RealPresence Access Director system.
Authentication error	<p>In the DMA system</p> <ul style="list-style-type: none"> • 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	<p>In the DMA system</p> <ul style="list-style-type: none"> • Go to Maintenance > Troubleshooting Utilities > Ping. • Check whether the RealPresence Access Director system is accessible. <p>On the inside firewall</p> <ul style="list-style-type: none"> • Check the firewall policy to determine if SIP ports are all permitted from untrust to trust zone. Default values are: <ul style="list-style-type: none"> – TCP: 5060, 5061 – UDP: 5060 <p>On the outside firewall</p> <ul style="list-style-type: none"> • 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	<p>On the caller and callee endpoints</p> <ul style="list-style-type: none"> • Check whether both the caller and the endpoint being called are registered. • Unregister and reregister the endpoint and call again.

Possible Reasons	Recommend Actions
Service network setting error	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • Go to the License Status pane on the Dashboard. • Check whether the Maximum Allowed Calls have been reached.
DMA configuration error	<p>In the DMA system, determine if the dial rule configurations are correct.</p>
SIP ALG	<ul style="list-style-type: none"> • Check whether SIP ALG is enabled on the home NAT and firewall. • Disable SIP ALG and try the call again.
Bandwidth limitation:	<p>Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system.</p> <ul style="list-style-type: none"> • Go to Configuration > Media Traversal Settings. • Increase bandwidth limitation values. • Try the call again.

H.323 Call Failed

Possible Reasons	Recommend Actions
H.323 component not running	In the RealPresence Access Director system <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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 DMA system and internal endpoints subnets are included in the CIDR address.
License limitation	In the RealPresence Access Director system <ul style="list-style-type: none"> • Go to the License Status pane on the Dashboard. • Check whether the Maximum Allowed Calls have been reached.
Network issue between the RealPresence Access Director system and the gatekeeper	In the DMA system <ul style="list-style-type: none"> • Go to Maintenance > Troubleshooting Utilities > Ping and check whether the RealPresence Access Director system is reachable.

Possible Reasons	Recommend Actions
H.225 port error	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> 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	<p>On the outside firewall</p> <ul style="list-style-type: none"> Check whether the public signaling IP address of the RealPresence Access Director system is mapped to its internal IP address. <p>On the outside and inside firewall</p> <ul style="list-style-type: none"> Check the firewall policy to determine if H.323 ports are permitted from untrust to trust zone. <ul style="list-style-type: none"> Default H.323 port is 1720.
DMA configuration error	<p>In the DMA system, determine if the dial rule configurations are correct.</p>
H.323 ALG	<ul style="list-style-type: none"> Check whether H.323 ALG is enabled on the home NAT and firewall. Disable H.323 ALG and try the call again.
Bandwidth limitation	<p>Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system.</p> <ul style="list-style-type: none"> Go to Configuration > Media Traversal Settings. Increase bandwidth limitation values. <p>Try the call again.</p>

VMR Call Failed

Possible Reasons	Recommend Actions
Call signaling error	<ul style="list-style-type: none"> • Check whether a SIP or H.323 P2P call works correctly. <ul style="list-style-type: none"> – If so, the RealPresence Access Director system, the 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 6-73 and “H.323 Call Failed” on page 6-75.
VMR configuration error	In the DMA system, determine if the VMR number is correct.
DMA configuration error	In the DMA system, determine if the dial rule configurations are correct.

No Audio, Video, or Content

Possible Reasons	Recommend Actions
Media relay component error	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Check whether the audio is mute on the endpoint. • Check whether the camera works correctly on the endpoint.

Possible Reasons	Recommend Actions
Service network setting	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Deployed behind Outside Firewall is selected. <p>Signaling relay address and Media relay address contain the public address of the RealPresence Access Director system mapping on a firewall.</p>
BFCP over UDP for content	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<p>On the outside firewall,</p> <ul style="list-style-type: none"> Check the firewall policy to determine if external media ports are permitted from untrust to trust zone. <ul style="list-style-type: none"> – UDP: 20001-40000 <p>On the inside firewall</p> <ul style="list-style-type: none"> Check the firewall policy to determine if internal media ports are permitted from trust to untrust zone. <ul style="list-style-type: none"> – UDP: 40001-60000

Failed to Connect to RealPresence Resource Manager

Possible Reasons	Recommend Actions
Login name/password error	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> Go to Admin > Polycom Management System. Check whether the login name and password are correct.

Possible Reasons	Recommend Actions
Network issue between the RealPresence Access Director system and the RealPresence Resource Manager system	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to Admin > Troubleshooting > Utilities > Test Network > Ping. • Check whether the RealPresence Access Director system is accessible.
Certificate check fails	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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	<p>In the RealPresence Access Director system</p> <ul style="list-style-type: none"> • 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	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to Admin > 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	<p>In the RealPresence Resource Manager system</p> <ul style="list-style-type: none"> • Go to User > Users. • Check whether the login name of the user is in the user list.

