Contents

Conventions Used in Polycom Guides ........................................... 8
  Information Elements .......................................................... 8
  Typographic Conventions ...................................................... 9

Before You Begin ................................................................. 10
  RealPresence Access Director System Editions ................................ 10
  Audience, Purpose, and Required Skills .................................... 10
  Related Documentation .......................................................... 10
  Get Help .............................................................................. 11
    Polycom and Partner Resources ............................................. 11
    The Polycom Community .................................................... 11

Overview of the Polycom® RealPresence® Access Director™ System ....... 12
  About the Polycom RealPresence Access Director System .................. 12
  Features and Capabilities ...................................................... 13
    Appliance Edition and Virtual Edition ..................................... 13
    SIP and H.323 Signaling ....................................................... 13
    Access Proxy ....................................................................... 13
    Media Relay ....................................................................... 14
    High Availability ................................................................ 14
    TURN Server ..................................................................... 14
    Security ............................................................................ 14
    Support for F5 Load Balancer ............................................... 14
    Operating System ............................................................... 14
    Endpoints (AVC and SVC) .................................................... 15

Getting Started with the RealPresence Access Director System ................ 15
  Log In to and Out of the System User Interface ............................ 15
  Automatically Send Usage Data ................................................. 16
  Change Your Password ........................................................... 17
  Customize the Dashboard ......................................................... 17
  Monitor System Alerts ............................................................ 19
  Work with Menus .................................................................. 23
Access Online Help ................................................................. 25

System Configuration ............................................................ 26
  Configure Time Settings ......................................................... 26
  Set the Time Zone ............................................................... 27
  Edit the Time Settings ......................................................... 27
  System Licensing ............................................................... 28
    Appliance Edition Licensing ................................................. 29
    Virtual Edition Licensing .................................................. 31
    High Availability Licensing ............................................... 32
  Configure Network Settings .................................................. 33
    Network Settings Overview ............................................... 33
    Network Interface Configurations ....................................... 36
    Configure Static Route Settings ......................................... 39
  Configure Two-System Tunnel Settings (Optional) ....................... 40
    Configure Network and Tunnel Settings ................................ 41
  Configure Access Proxy Settings ............................................ 45
    Add a New Proxy Configuration .......................................... 47
    Configure HTTPS Proxy Settings ....................................... 47
    Configure LDAP Proxy Settings ......................................... 50
    Configure XMPP Proxy Settings ........................................ 51
    Configure a Passthrough Proxy ......................................... 52
    Configure HTTP Tunnel Settings ....................................... 53
    Edit Proxy Settings ....................................................... 54
    Delete Proxy Configurations .......................................... 55
  Configure Basic Access Control List Settings ............................ 55
    How Basic ACLs Work ..................................................... 56
    Configure Registration Policy Settings ................................ 56
    Configure Call Policy Settings ......................................... 59
  Manage Certificates ........................................................... 61
    How Certificates Are Used ............................................... 62
    Accepted Forms of Certificates ........................................ 62
    Certificate Procedures ................................................... 63
    View Installed Certificates ............................................. 63
    View Certificate Details .................................................. 64
    Use the Online Certificate Status Protocol ............................ 66
    Add a Certificate Authority’s Public Certificate ....................... 66
    Create a Certificate Signing Request ................................... 67
    Review the Signed Certificate ......................................... 69
    Add the Signed Certificate to the KEY_STORE .......................... 70
### System Administration and Additional Settings 92

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability Settings</td>
<td>92</td>
</tr>
<tr>
<td>Configure High Availability Settings</td>
<td>93</td>
</tr>
<tr>
<td>Change HA Password</td>
<td>95</td>
</tr>
<tr>
<td>View High Availability Status Details</td>
<td>95</td>
</tr>
<tr>
<td>Set Custom Security for Network Access</td>
<td>95</td>
</tr>
<tr>
<td>Configure Port Range Settings</td>
<td>96</td>
</tr>
<tr>
<td>Configure Log Settings</td>
<td>98</td>
</tr>
<tr>
<td>Configure Log File Rolling and Application Log Settings</td>
<td>99</td>
</tr>
<tr>
<td>Configure Remote Syslog Settings</td>
<td>100</td>
</tr>
<tr>
<td>SNMP Overview</td>
<td>101</td>
</tr>
<tr>
<td>SNMP Framework</td>
<td>101</td>
</tr>
<tr>
<td>SNMP Versions</td>
<td>101</td>
</tr>
<tr>
<td>SNMP Notifications</td>
<td>102</td>
</tr>
<tr>
<td>Configure SNMP Settings</td>
<td>103</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configure Notification Users</td>
<td>104</td>
</tr>
<tr>
<td>Configure Notification Agents</td>
<td>105</td>
</tr>
<tr>
<td>Download MIBs</td>
<td>107</td>
</tr>
<tr>
<td>Configure History Retention Settings</td>
<td>107</td>
</tr>
<tr>
<td>Define Advanced Access Control List Rules</td>
<td>109</td>
</tr>
<tr>
<td>Use the Default Access Control List Rules</td>
<td>110</td>
</tr>
<tr>
<td>Add an Access Control List Rule and Conditions</td>
<td>113</td>
</tr>
<tr>
<td>Copy an Access Control List Rule</td>
<td>114</td>
</tr>
<tr>
<td>Edit or Delete an Access Control List Rule</td>
<td>114</td>
</tr>
<tr>
<td>Edit or Delete a Condition for an Access Control List Rule</td>
<td>115</td>
</tr>
<tr>
<td>Example: Define an Access Control List Rule to Deny SIP Calls from Specific IP Addresses</td>
<td>115</td>
</tr>
<tr>
<td>Use Variables in Access Control List Rules</td>
<td>116</td>
</tr>
<tr>
<td>Add a Variable</td>
<td>117</td>
</tr>
<tr>
<td>Edit or Delete a Variable</td>
<td>117</td>
</tr>
<tr>
<td>Apply Rule Settings to Access Control List Rules</td>
<td>118</td>
</tr>
<tr>
<td>Add an Access Control List Setting and Rule Setting</td>
<td>118</td>
</tr>
<tr>
<td>Edit or Delete an Access Control List Setting</td>
<td>119</td>
</tr>
<tr>
<td>Edit or Delete a Rule Setting</td>
<td>119</td>
</tr>
<tr>
<td>Use Management</td>
<td>121</td>
</tr>
<tr>
<td>Manage Local User Accounts and User Roles</td>
<td>121</td>
</tr>
<tr>
<td>Change Your System Password</td>
<td>121</td>
</tr>
<tr>
<td>Search for a Local User Account</td>
<td>122</td>
</tr>
<tr>
<td>Add a Local User Account and Assign User Roles</td>
<td>122</td>
</tr>
<tr>
<td>Edit and Delete Local User Account Information</td>
<td>123</td>
</tr>
<tr>
<td>System Maintenance</td>
<td>125</td>
</tr>
<tr>
<td>Upgrade the Software</td>
<td>125</td>
</tr>
<tr>
<td>View Software Information</td>
<td>125</td>
</tr>
<tr>
<td>Upload an Upgrade Package File</td>
<td>126</td>
</tr>
<tr>
<td>Install an Uploaded Package File</td>
<td>126</td>
</tr>
<tr>
<td>Upload and Upgrade at the Same Time</td>
<td>127</td>
</tr>
<tr>
<td>Roll Back to the Previous Software Version</td>
<td>127</td>
</tr>
<tr>
<td>Shut Down and Restart the System</td>
<td>128</td>
</tr>
<tr>
<td>Back Up and Restore the System</td>
<td>128</td>
</tr>
<tr>
<td>Create a Backup File</td>
<td>129</td>
</tr>
<tr>
<td>Download a Backup File</td>
<td>129</td>
</tr>
<tr>
<td>Upload a Backup File</td>
<td>130</td>
</tr>
<tr>
<td>Restore the System from a Backup File</td>
<td>130</td>
</tr>
<tr>
<td>Remove a Backup File</td>
<td>130</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Migrate Data from a Backup File</td>
<td>131</td>
</tr>
<tr>
<td><strong>System Diagnostics</strong></td>
<td>133</td>
</tr>
<tr>
<td>View Active Call Details</td>
<td>133</td>
</tr>
<tr>
<td>Call History</td>
<td>134</td>
</tr>
<tr>
<td>Search for Call Records</td>
<td>134</td>
</tr>
<tr>
<td>View Call Details</td>
<td>134</td>
</tr>
<tr>
<td>Audit Registration History</td>
<td>136</td>
</tr>
<tr>
<td>Search for Registration Records</td>
<td>136</td>
</tr>
<tr>
<td>View Registration Details</td>
<td>136</td>
</tr>
<tr>
<td>View TURN Allocations</td>
<td>138</td>
</tr>
<tr>
<td>Manage System Log Files</td>
<td>139</td>
</tr>
<tr>
<td>View the Disposition for SIP and H.323 Calls</td>
<td>139</td>
</tr>
<tr>
<td>Download Log Files</td>
<td>140</td>
</tr>
<tr>
<td>Delete Log Files</td>
<td>140</td>
</tr>
<tr>
<td>Roll Log Files</td>
<td>141</td>
</tr>
<tr>
<td>Run Traffic Capture</td>
<td>141</td>
</tr>
<tr>
<td>Ping a Device</td>
<td>142</td>
</tr>
<tr>
<td>Run Traceroute</td>
<td>142</td>
</tr>
<tr>
<td>View High Availability Status</td>
<td>142</td>
</tr>
<tr>
<td>Use Polycom Utilities</td>
<td>143</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>144</td>
</tr>
<tr>
<td>Remote Client Login Failed</td>
<td>145</td>
</tr>
<tr>
<td>Licensed Call Number is 0</td>
<td>146</td>
</tr>
<tr>
<td>SIP Registration Failed</td>
<td>146</td>
</tr>
<tr>
<td>SIP Call Failed</td>
<td>148</td>
</tr>
<tr>
<td>H.323 Call Failed</td>
<td>149</td>
</tr>
<tr>
<td>VMR Call Failed</td>
<td>150</td>
</tr>
<tr>
<td>No Audio, Video, or Content</td>
<td>150</td>
</tr>
<tr>
<td>Failed to Connect to RealPresence Resource Manager System</td>
<td>151</td>
</tr>
<tr>
<td>Cannot Open RealPresence Access Director System User Interface</td>
<td>152</td>
</tr>
</tbody>
</table>
Conventions Used in Polycom Guides

This guide contains terms, graphical elements, and a few typographic conventions. Familiarizing yourself with these terms, elements, and conventions will help you successfully perform tasks.

Information Elements

This guide may include any of the following icons to alert you to important information.

Icons Used in this Guide

<table>
<thead>
<tr>
<th>Name</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>![Note Icon]</td>
<td>The Note icon highlights information of interest or important information needed to be successful in accomplishing a procedure or to understand a concept.</td>
</tr>
<tr>
<td>Caution</td>
<td>![Caution Icon]</td>
<td>The Caution icon highlights information you need to know to avoid a hazard that could potentially impact device performance, application functionality, or successful feature configuration.</td>
</tr>
<tr>
<td>Warning</td>
<td>![Warning Icon]</td>
<td>The Warning icon highlights an action you must perform (or avoid) to prevent issues that may cause you to lose information or your configuration setup, and/or affect phone, video, or network performance.</td>
</tr>
<tr>
<td>Web Info</td>
<td>![Web Info Icon]</td>
<td>The Web Info icon highlights supplementary information available online such as documents or downloads on support.polycom.com or other locations.</td>
</tr>
<tr>
<td>Administrator Tip</td>
<td>![Administrator Tip Icon]</td>
<td>The Administrator Tip icon highlights techniques, shortcuts, or productivity related tips.</td>
</tr>
<tr>
<td>User Tip</td>
<td>![User Tip Icon]</td>
<td>The User Tip icon highlights techniques, shortcuts, or productivity related tips.</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>![Troubleshooting Icon]</td>
<td>The Troubleshooting icon highlights information that may help you solve a relevant problem or to refer you to other relevant troubleshooting resources.</td>
</tr>
</tbody>
</table>
Typographic Conventions

A few typographic conventions, listed next, may be used in this guide to distinguish types of in-text information.

### Typographic Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Highlights interface items such as menus, menu selections, window and dialog names, soft keys, file names, and directory names when they are involved in a procedure or user action. Also used to highlight text to be entered or typed.</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Used to emphasize text, to show example values or inputs (in this form: <code>&lt;example&gt;</code>), and to show titles of reference documents available from the Polycom Support Web site and other reference sites.</td>
</tr>
<tr>
<td><strong>Blue Text</strong></td>
<td>Used for cross references to other sections within this document and for hyperlinks to external sites and documents.</td>
</tr>
<tr>
<td><strong>Courier</strong></td>
<td>Used for code fragments and parameter names.</td>
</tr>
</tbody>
</table>
Before You Begin

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

RealPresence Access Director System Editions

The RealPresence Access Director system is available in an Appliance Edition (packaged with a system server) and a Virtual Edition (packaged as software only). Most of the functionality described in this document applies to both editions, and so the product references are general—that is, the RealPresence Access Director system. However, when information applies to a specific edition, the reference will be the RealPresence Access Director, Virtual Edition, or the RealPresence Access Director, Appliance Edition.

Audience, Purpose, and Required Skills

This content is written for a technical audience. As a system administrator of the RealPresence Access Director system, you should have knowledge and skills in the following areas:

- Computer and network system administration
- Network configuration, including IP addressing, subnets, gateways, domains, DNS, certificates, time servers, and possibly network routing rules
- Firewalls and network security
- Virtual infrastructures and cloud computing (Virtual Edition)
- The deployment model for the RealPresence Access Director system being installed and the video conferencing/collaboration network of which it will be a part

If necessary, obtain the assistance of the appropriate IT or network administration personnel before using the RealPresence Access Director system.

Related Documentation

Please read all available documentation before you install or operate the system. Documents are available at Documents and Downloads at Polycom Support.

- Polycom RealPresence Access Director System Release Notes
- Polycom RealPresence Access Director Getting Started Guide
- Polycom Unified Communications in RealPresence Access Director System Environments
Get Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

Polycom and Partner Resources

To find all Polycom partner solutions, see Strategic Global Partner Solutions.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, simply create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.
Overview of the Polycom® RealPresence® Access Director™ System

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

- About the Polycom RealPresence Access Director System
- Features and Capabilities
- Getting Started with the RealPresence Access Director System

About the Polycom RealPresence Access Director System

The RealPresence Access Director system enables users within and beyond your firewall to securely access voice, video, and multimedia sessions across IP network borders. The system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP and H.323 video calls (including H.460 firewall/NAT traversal) from registered users, guests, and federated enterprises or divisions.

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

- Polycom RealPresence Resource Manager system – provides management, provisioning, directory, and presence services
- Polycom RealPresence Distributed Media Application™ (DMA®) system – serves as a central call control platform for SIP, H.323, and bridge virtualization, and act as H.323 gatekeepers
- Polycom RealPresence Collaboration Server system – serves as a high-scale bridge for SIP and H.323 calls and supports content over video
- Polycom RealPresence One solution – combines the complete Platform with software endpoints and optimized services
- Polycom RealPresence Web Suite – pure software extension of the RealPresence Platform that provides universal access to video conferencing, independent of application, system, or device
- Polycom RealPresence Platform Director™ solution – provides the ability to deploy the software and manage the licensing of RealPresence Platform, Virtual Edition products in an organization’s data center or in the cloud
- Polycom RSS™ recording and streaming server – enables recording of video, audio, and content
- Polycom RealPresence Desktop software – supports sharing of video, audio, and content from your desk
- Polycom RealPresence Mobile software – enables tablets and smartphones to connect to video and audio conferencing and to share content
Polycom ContentConnect™ system – connects Lync desktop workers, conference room systems, and audio-only meeting participants for video collaboration
- Polycom RealPresence Group Series 300/500 video collaboration solution – endpoints that support large-scale video conferencing
- Polycom HDX group video system – endpoints that provide high-definition video and voice for video conferencing
- Cisco codecs and desktop systems (some models)

Features and Capabilities
The RealPresence Access Director system provides the key features described below.

Appliance Edition and Virtual Edition
The RealPresence Access Director system is available in an Appliance Edition (packaged with a system server for an appliance-based infrastructure) and a Virtual Edition (packaged as software only for a virtual environment). Both editions provide the same firewall traversal functionality and can be integrated with other RealPresence Platform components to provide a seamless video collaboration experience.

SIP and H.323 Signaling
The RealPresence Access Director system provides connectivity for SIP (both SVC and AVC) or H.323 users, enabling them to securely collaborate over video from different locations and devices. Specifically, the RealPresence Access Director system enables:
- SIP and H.323 remote users (registered/provisioned endpoints) to securely connect to your enterprise network as managed users, with the same functionality they would have if they were inside your enterprise network firewall
- SIP and H.323 guest users (unregistered/unprovisioned endpoints, such as customers, partners, and vendors) to securely connect to your enterprise network
- SIP and H.323 B2B calling through trusted (federated or neighbored) connections to other enterprises’ networks
- Open SIP and H.323 calling to and from users outside your network
- SIP RealPresence Web Suite guest users with browser-based clients to connect to RealPresence Web Suite video conferences within your enterprise network (The HTTPS tunnel proxy does not support SVC video conferencing.)

Access Proxy
The access proxy feature provides reverse proxy functionality that enables external endpoints to access services inside your enterprise network. Registered (remote) users can access the following services:
- Management and provisioning (HTTPS/TLS)
- Presence (XMPP/TLS)
- Directory (LDAP/TLS)

Additionally, an HTTP tunnel can be configured to enable RealPresence Web Suite SIP guest users to join meetings inside the enterprise network (through the RealPresence Web Suite Services Portal).
Media Relay
The RealPresence Access Director system supports the media connection between external users and enterprise users. This connection enables audio, video, and content relay over UDP media channels.

High Availability
Two RealPresence Access Director systems can be configured on the same network to provide High Availability (HA) of services. Systems configured for High Availability support minimal interruption of services and greater call reliability.

TURN Server
To support WebRTC-based video conferencing, the RealPresence Access Director system implements both Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols. When needed, the RealPresence Access Director system can act as a STUN and TURN server to enable firewall and NAT traversal of UDP media traffic between WebRTC clients.

Security
To provide secure firewall traversal for video calls, the RealPresence Access Director system provides the following security features:

- Deployment behind outside firewalls that use Network Address Translation (NAT)
- Secured communications (TLS and certificates)
- Secure management (Access Control Lists, Syslog, LDAP authentication, and role-based access control)
- Server-side authentication
- Server-side session management
- Robust SIP TLS cipher
- OS hardening

Support for F5 Load Balancer
Two or more RealPresence Access Director systems can be deployed behind an F5 Networks load balancer to increase network capacity (concurrent users) and improve overall performance by decreasing the burden on any one RealPresence Access Director system.

The F5 load balancer acts as a TCP or UDP reverse proxy to distribute (balance) incoming sign-in, registration, and call requests across multiple RealPresence Access Director systems. When the F5 load balancer receives a request, it distributes that request to a particular RealPresence Access Director system. An F5 load balancer can help to ensure RealPresence Access Director system reliability and availability by sending requests only to systems that can respond in a timely manner.

See Polycom Unified Communications in RealPresence Access Director System Environments for instructions on integrating an F5 load balancer with RealPresence Access Director systems.

Operating System
The system uses the hardened CentOS 6.6 operating system platform.
Endpoints (AVC and SVC)

The RealPresence Access Director system supports calls to and from the following endpoints:

- RealPresence Group Series 300/500
- RealPresence Mobile
- RealPresence Desktop
- Polycom HDX systems
- Cisco C20 and C40 Codecs, EX60 and EX90 Desktop Systems, and 1700 MXP Desktop System (AVC only)

Getting Started with the RealPresence Access Director System

The following topics provide general instructions for using the RealPresence Access Director system:

- Log In to and Out of the System User Interface
- Automatically Send Usage Data
- Change Your Password
- Customize the Dashboard
- Monitor System Alerts
- Work with Menus
- Access Online Help

Log In to and Out of the System User Interface

The RealPresence Access Director system provides a web user interface to configure, manage, and monitor the system.

Caution: Use the correct login credentials

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

To log in and out of the RealPresence Access Director user interface:

1. Open a browser window and in the Address field, do one of the following:
   - If you specified your system IP address during initial installation and network configuration, enter your IP address.
   - If you did not specify your system IP address during initial installation and network configuration, enter the RealPresence Access Director default IP address:
     https://192.168.1.254:8443

2. In the Log In screen, enter the following:
   - User ID: admin
Password: Polycom12#$

The user ID admin and password Polycom12#$ are the default login credentials after the initial installation of the system. If you have created other user accounts, the user logging in must use their own credentials.

3 Click in the top-right corner of the page to log out of the system.

Automatically Send Usage Data

To continually improve the product, it is important to gain understanding of how the RealPresence Access Director system is used by customers. By collecting this data, Polycom can identify both the system level utilization and the combination and usage of RealPresence Access Director system features. This usage data will inform Polycom which features are important and are actually used on your system. Polycom will use this information to help guide future development and testing to concentrate on the areas of Access Director that are most heavily used. If you choose not to send this information, Polycom is less aware of which features are important to you and that are used by you, which may influence future development to go in directions that are less beneficial to you.

Your decision to enable or not enable the sending of this data does not affect the availability of any documented system feature in any way. Enabling this feature does not affect the capacity or responsiveness of the RealPresence Access Director system to process calls, conferences, GUI or API interactions.

The system sends the data once per hour over a secured (TLS) connection to a Polycom collection point (customerusagedatacollection.polycom.com). There is no access by any customer or others to view the data received at the collection point. The raw data will be viewable only by Polycom. To avoid any impact to starting and ending calls and conferences, data is never sent between 5 minutes before the hour and 5 minutes after the hour.

The following types of data are reported:

- License information
- Hardware configuration
- System resource usage: CPU, RAM, disk, database
- System configuration: number of servers, clusters
- Feature configuration: Enterprise Directory Integration, Lync, Dial Rules, Shared Number Dialing, Hunt Groups, Registration Policy, Device Authentication
- Number of users, endpoints, sites, MCUs, external gatekeepers, SIP peers, SBCs
- Registrations, call and conference statistics
- Security settings

When this information is reported, a customer’s user and environment identifying information (e.g., internal IP addresses and FQDNs, names of users, devices, external systems, etc.) is made anonymous before being sent from the system. System serial numbers and license information are sent without anonymization and may be used to help improve customer experiences. In total, less than 100KB of data per hour is collected and sent.

Polycom’s collection and use of this data complies with Polycom’s Privacy Policy.

Enable or Disable Automatic Data Collection

Initially, you can decide to allow or disallow the automatic sending of usage data when the system’s End User License Agreement is presented.
You can view and change the current status of usage data sending and collection on the **Maintenance > License** page. Usage data is sent only if the **Automatically send usage data** field is checked. You can enable or disable this feature at any time.

**View the Collected Usage Data**

The system records data that has been sent and collected in the system logs.

**To view the collected usage data:**

1. Log in to the RealPresence Access Director system as an Administrator.
2. Download the system logs. See **Download Log Files**.
3. On the PC where the logs have been downloaded, use an archiving or zipping tool to extract the file `analytics.json`.
   Analytics.json is a text file containing the hourly data reported most recently before the time when the system logs were created.
4. View the analytics.json file with Notepad or another common text editing tool.

**Change Your Password**

Polycom recommends that users change their passwords at least once every 60 days.

**To change your system password:**

1. Go to **User > Users**.
2. Select your account from the list of users.
3. Under **Actions**, click **Edit**.
4. Enter your new password in the **Password** and **Confirm Password** fields, according to the following requirements:
   - The password length must be 9–20 characters.
   - The password must contain at least one upper case letter, one lower case letter, and one number.
5. Click **OK**.

**Customize 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 the panes you want to view. The system saves your settings for subsequent logins.

The following dashboard panes are available:

- **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 or stopped:
  - Access Proxy
  - SIP
  - H323
  - TURN server
  - Media Relay
  - Two-box Tunnel (the tunnel service status displays only if you deploy two RealPresence Access Director systems in a tunnel configuration.)
  - Database
- **License Status.** This pane displays license server connection, call, and bandwidth information:
  - Last successful connection (Virtual Edition only)
  - Maximum Allowed Calls
  - Active SIP Calls
  - Active H.323 Calls
  - Active SIP Bandwidth
  - Active H.323 Bandwidth
- **Peak Call Monitoring.** This pane displays the percentage of active SIP and H.323 calls.
- **TURN Status.** This pane displays whether the TURN server is running, the number of allocations, and the total bandwidth that the TURN server is using.
- **High Availability Status.** If you have two RealPresence Access Director systems configured to provide High Availability, this pane displays the connection status of both systems and network interface IP addresses, address types, and state information:

**To add panes to the dashboard:**
1. Click *Add Panes*.
2. From the menu, select the panes you want to display.

**To close or resize a pane:**
1. Click X.
2. Click to maximize.
3. Click to restore the default size.

**To set the refresh interval for the dashboard display:**
» Click the down arrow on the *Refresh Every 15 seconds* button and select a refresh interval.
   The dashboard refreshes based on the interval you select.

**To return to the dashboard from other functions:**
» Click .
Monitor System Alerts

In addition to the dashboard panes, the System Alerts lists alerts about system certificates (Appliance Edition and Virtual Edition) and licensing (Virtual Edition only). These alerts display when:

- Certificates are close to their expiration date or have expired.
- License information for the Virtual Edition changes, including the number of licensed calls, access to features, and license status (that is, active or expired).

When alerts occur, the System Alerts button turns red and displays the current number of alerts. Each alert has a corresponding severity level:

- **Warn**—The system currently functions correctly, but Polycom recommends that you resolve the issue identified in the alert before it becomes severe.
- **Severe**—The system temporarily does not function correctly. The system may recover automatically but Polycom recommends that you resolve the issue before it becomes critical.
- **Critical**—The system does not function correctly. Resolve the issue immediately.

To open and close the System Alerts pane:

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

The following table defines the certificate and Virtual Edition license issues that may trigger an alert and the action to take to resolve an issue.

<table>
<thead>
<tr>
<th>Alert Description</th>
<th>Severity</th>
<th>Reason for Alert</th>
<th>Action to Resolve the Issue</th>
</tr>
</thead>
</table>
| Expires within 30 days. Upon expiration, encrypted calls or communication with other servers may be blocked. | Warn       | The key store certificate will expire within 30 days.                             | - Go to Admin > Certificates.  
- Click Refresh next to the key store certificate.  
**Note:** The key store certificate is replaced with a new self-signed certificate. You must submit a new certificate signing request to your trusted CA to obtain a new signed certificate. |
<p>| Expires within 30 days. Upon expiration, all system access may be lost.           | Warn       | The trusted certificate will expire within 30 days.                             | Install trusted certificates from the appropriate source, for example an internal or external CA, a TLS peer, etc. |</p>
<table>
<thead>
<tr>
<th>Alert</th>
<th>Severity Level</th>
<th>Reason for Alert</th>
<th>Action to Resolve the Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expired. Encrypted calls or communication with other servers may be blocked.</td>
<td>Critical</td>
<td>The key store certificate expires while the RealPresence Access Director system is running.</td>
<td>Restart the system and it automatically generates a new self-signed certificate. <strong>Note:</strong> If the key store certificate expires when the RealPresence Access Director system is not running, the system automatically generates a new self-signed certificate when the system is started again. No alert displays.</td>
</tr>
<tr>
<td>Expired. Encrypted calls or communication with other servers may be blocked.</td>
<td>Critical</td>
<td>The trusted certificate has expired.</td>
<td>Immediately submit a new CSR.</td>
</tr>
</tbody>
</table>

**Licenses (Virtual Edition only)**

| Connection to the license server successful | Warn | The RealPresence Access Director system successfully connects to the license server after failing to connect on the last attempt. | N/A |
| The license server's configuration is incorrect | Warn | The license server configuration is incorrect or missing information. For example, the license server IP address has not been specified. | Go to **Maintenance > License Server Settings** and check the license server IP address and port for incorrect or missing information. Revise incorrect settings in the RealPresence Platform Director user interface. |
| The base license for RealPresence Access Director has changed. Restart the system. | Severe | The base license for the RealPresence Access Director system has changed. For example:  
  • The license was valid but has now expired.  
  • The license was not available from the license server but has now been retrieved and validated. | When the base license for the RealPresence Access Director system changes from valid to invalid, the RealPresence Access Director system responds as follows:  
  • If active calls are in progress, the system automatically restarts after all active calls have ended.  
  • If no active calls are in progress, the system automatically restarts.  
When an invalid base license becomes valid, the system automatically restarts. **Note:** In a two-system tunnel configuration, if the tunnel client is running, you must manually restart it. |
<table>
<thead>
<tr>
<th>Alert</th>
<th>Severity Level</th>
<th>Reason for Alert</th>
<th>Action to Resolve the Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot acquire the base license for the RealPresence Access Director system.</td>
<td>Critical</td>
<td>The system cannot acquire the base license for the RealPresence Access Director system from the license server. In such cases, all RealPresence Access Director system functions are disabled.</td>
<td>In RealPresence Platform Director, ensure that the RealPresence Access Director base license is correctly configured. The RealPresence Access Director system will connect to the license server every one minute to attempt to acquire the base license.</td>
</tr>
<tr>
<td>The maximum call count on the license exceeds system capability.</td>
<td>Severe</td>
<td>The maximum number of calls on the Max Calls for RealPresence Access Director license exceeds system capabilities. If the licensed call number configured in the RealPresence Platform Director system is higher than the maximum number of calls the RealPresence Access Director system supports, the additional calls are not supported.</td>
<td>Ensure that the maximum number of calls on the Max Calls for RealPresence Access Director license does not exceed system capabilities.</td>
</tr>
<tr>
<td>The number of licensed calls has changed from &lt;number X&gt; to &lt;number Y&gt;. Restart the system, then confirm the new port ranges.</td>
<td>Critical</td>
<td>The licensed call number on the Max Calls for RealPresence Access Director license changes on the license server.</td>
<td>Manually restart the RealPresence Access Director system. Then go to Admin &gt; Port Range Settings and view the new port ranges. Ensure that the ports configured on the firewall match the new port ranges.</td>
</tr>
<tr>
<td>Alert</td>
<td>Severity Level</td>
<td>Reason for Alert</td>
<td>Action to Resolve the Issue</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>The media encryption license has changed. Restart the system.</td>
<td>Severe</td>
<td>If two RealPresence Access Director systems have been deployed in a tunnel configuration, encrypting the tunnel between the two systems is possible only with the Enable Strong Media Encryption license capability. The alert displays if tunnel encryption is enabled and the Enable Strong Media Encryption capability changes on the license server.</td>
<td>When the Enable Strong Media Encryption license capability changes, the RealPresence Access Director system responds as follows: <strong>Tunnel Server</strong> If active calls are in progress, the tunnel server does not automatically restart. If not calls are in progress, the tunnel server responds as follows: • If the tunnel is running in encrypted mode, the tunnel server automatically restarts in unencrypted mode. • If the tunnel is running in unencrypted mode and the tunnel settings have been configured as unencrypted in the RealPresence Access Director system's user interface, the tunnel server continues to operate without interruption. • If the tunnel is running in unencrypted mode and the tunnel settings have been configured as encrypted in the RealPresence Access Director system's user interface, the tunnel server automatically restarts in encrypted mode. <strong>Tunnel Client</strong> If the tunnel client is running, it does not restart. If it is not running, it will automatically restart and reconnect to the tunnel server.</td>
</tr>
</tbody>
</table>
To open and close the System Alerts pane:

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

Work with Menus

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

When configuring RealPresence Access Director system settings, all required fields display a red asterisk (*) next to the field name.

The following table lists all of the menus and their corresponding functions (submenus). Note that some submenu names differ slightly between the RealPresence Access Director, Appliance Edition, and the RealPresence Access Director, Virtual Edition.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Submenu</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Proxy Settings</td>
</tr>
<tr>
<td>Menu</td>
<td>Submenu</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>SIP Settings</td>
<td></td>
</tr>
<tr>
<td>H.323 Settings</td>
<td></td>
</tr>
<tr>
<td>TURN Settings</td>
<td></td>
</tr>
<tr>
<td>Media Traversal Settings</td>
<td></td>
</tr>
<tr>
<td>Federation Settings</td>
<td></td>
</tr>
<tr>
<td>Two-box Tunnel Settings</td>
<td></td>
</tr>
<tr>
<td>Basic ACL Settings</td>
<td></td>
</tr>
<tr>
<td>Advanced ACL Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control List Rules</td>
</tr>
<tr>
<td></td>
<td>Access Control List Variables</td>
</tr>
<tr>
<td></td>
<td>Access Control List Settings</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>License</td>
<td></td>
</tr>
<tr>
<td>Software Upgrade</td>
<td></td>
</tr>
<tr>
<td>Shutdown and Restart</td>
<td></td>
</tr>
<tr>
<td>Backup and Restore</td>
<td></td>
</tr>
<tr>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>Network Settings</td>
<td></td>
</tr>
<tr>
<td>Time Settings</td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td></td>
</tr>
<tr>
<td>Security Settings</td>
<td></td>
</tr>
<tr>
<td>Log Settings</td>
<td></td>
</tr>
<tr>
<td>SNMP Settings</td>
<td></td>
</tr>
<tr>
<td>History Retention Settings</td>
<td></td>
</tr>
<tr>
<td>Port Range Settings</td>
<td></td>
</tr>
<tr>
<td>High Availability Settings</td>
<td></td>
</tr>
<tr>
<td>Polycom Management System</td>
<td></td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td></td>
</tr>
<tr>
<td>Diagnostics</td>
<td></td>
</tr>
<tr>
<td>Active Calls</td>
<td></td>
</tr>
<tr>
<td>Call History</td>
<td></td>
</tr>
</tbody>
</table>
Access Online Help

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

- When you select a function from one of the menus, click the help icon at the top of page to access the help contents for that page.
- Within a window that requires you to enter information, click Help to display the specific help contents for that window.
- Open Help Contents to view a full listing of help topics.

To use the online help:

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

Note: Two-system tunnel user interfaces differ

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Submenu</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Registration History</td>
</tr>
<tr>
<td></td>
<td>TURN Allocations</td>
</tr>
<tr>
<td></td>
<td>System Log Files</td>
</tr>
<tr>
<td></td>
<td>Traffic Capture</td>
</tr>
<tr>
<td></td>
<td>Ping</td>
</tr>
<tr>
<td></td>
<td>Traceroute</td>
</tr>
<tr>
<td></td>
<td>High Availability Status</td>
</tr>
<tr>
<td>Help</td>
<td>About RPAD</td>
</tr>
<tr>
<td></td>
<td>Help Contents</td>
</tr>
</tbody>
</table>

Menu | Submenu
--- | ---
Registration History
TURN Allocations
System Log Files
Traffic Capture
Ping
Traceroute
High Availability Status

Help
About RPAD
Help Contents

Note: Two-system tunnel user interfaces differ

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

Access Online Help

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

- When you select a function from one of the menus, click the help icon at the top of page to access the help contents for that page.
- Within a window that requires you to enter information, click Help to display the specific help contents for that window.
- Open Help Contents to view a full listing of help topics.

To use the online help:

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

Note: Two-system tunnel user interfaces differ

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

Access Online Help

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

- When you select a function from one of the menus, click the help icon at the top of page to access the help contents for that page.
- Within a window that requires you to enter information, click Help to display the specific help contents for that window.
- Open Help Contents to view a full listing of help topics.

To use the online help:

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

After you have installed the Polycom® RealPresence® Access Director™ system and entered the initial network settings, you will need to configure several key system settings, as discussed in the sections that follow. Additionally, you can revise your system settings as needed after the initial configuration.

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

- Configure Time Settings
- System Licensing
- Configure Network Settings
- Configure Two-System Tunnel Settings (Optional)
- Configure Access Proxy Settings
- Configure Basic Access Control List Settings
- Manage Certificates
- Provision the System
- Integrate with Microsoft Active Directory
- Configure SIP Signaling Settings
- Configure H.323 Signaling Settings
- TURN Services
- Configure Media Traversal Settings
- Configure Federation Settings

For information on installation and initial system configuration, see the Polycom RealPresence Access Director, Appliance Edition or Virtual Edition, Getting Started Guide.

For system deployment information, see Polycom Unified Communications in RealPresence Access Director System Environments. Both documents are available at support.polycom.com.

Configure Time Settings

From the Time Settings page, you can configure time settings after the initial installation of your system and edit the system time and time zone when necessary.

Note: Configure NTP server IP addresses for the Virtual Edition

If you deploy an instance of the RealPresence Access Director system, Virtual Edition, Polycom recommends that you configure two Network Time Protocol (NTP) server IP addresses from the Polycom® RealPresence® Platform Director™ system user interface.
Consider the following information before changing the time settings:

- If you deploy an instance of the RealPresence Access Director system, Virtual Edition, the system time synchronizes with the NTP servers you configured from the RealPresence Platform Director system user interface.
- Changing the time settings requires a system restart, which terminates active calls and logs all users out of the system.
- Changing the time settings can affect the number of days available for a trial period license.
- If you plan to install an identity certificate provided by a certificate authority (CA), the date, time, and time zone configured in your system must be correct for the certificate to function correctly. See Manage Certificates for more information on certificates.
- If you plan to use your system to support calls between endpoints in your enterprise and endpoints in a separate but federated or neighbored (trusted) division or enterprise that has its own RealPresence Access Director system installed, both systems and the CA server should be in the same time zone. If the time difference between the two RealPresence Access Director systems and the CA server is too great, Transport Layer Security (TLS) connections may fail.

**Set the Time Zone**

After initial installation of the RealPresence Access Director system, the default time zone is GMT (UTC). When you launch the system for the first time, you must specify the time zone of your geographic location. Polycom strongly recommends that you select the time zone of your specific geographic location (for example, America/Denver) instead of a generic GMT offset (such as GMT+7).

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

**To set the time zone:**

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

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

**Edit 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: Server Time (Refresh every 10 seconds) indicates the server time. If you change the System time zone or Manually set the system time (not recommended), the Server Time (Refresh every 10 seconds) field displays the correct server time.
To edit the time settings:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System time zone</td>
<td>The time zone in which your RealPresence Access Director system is located. Note: After initial installation of the RealPresence Access Director system, the default time zone is GMT (UTC). You must select the time zone of your geographic location immediately after installing the system.</td>
</tr>
<tr>
<td>Auto adjust for Daylight Saving Time</td>
<td>Automatically determined in accordance with the system time zone. If the system time zone you select observes Daylight Saving Time, this setting is enabled. Note: The administrator cannot change this setting.</td>
</tr>
<tr>
<td>Manually set system time</td>
<td>Polycom strongly recommends that you do not set the time and date manually. Manually setting system time removes Network Time Protocol (NTP) server information and sets the manually entered time for the selected time zone instead of for the current system UTC offset.</td>
</tr>
<tr>
<td>NTP servers</td>
<td>The IP addresses or FQDNs of the NTP servers. • For Appliance Editions, the NTP server IP addresses may be provisioned by the Polycom® RealPresence® Resource Manager system or you can enter them manually. • For Virtual Editions, you can configure up to three NTP servers when you create an instance of the RealPresence Access Director system from the RealPresence Platform Director system. You can later edit these server addresses as needed. Note: Polycom recommends that you specify at least two NTP servers for synchronizing system time.</td>
</tr>
</tbody>
</table>

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.

**Caution: Changing time settings requires a system restart**

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

---

**System Licensing**

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

The RealPresence Access Director system automatically calculates dynamic port ranges based on the number of calls for which you are licensed. A port range for a specific function indicates the number of ports for that function that must be available to accommodate the number of calls on your system license. If your
number of licensed calls changes, after your system restarts, you must reconfigure your dynamic port range settings and make the corresponding changes on your firewall. See Configure Port Range Settings.

**Appliance Edition Licensing**

With your RealPresence Access Director product order, you will receive a License Certificate that includes a license number. Additionally, each new RealPresence Access Director, Appliance Edition server comes with a trial period license for five concurrent calls, to be used within 60 days after your system software is initially installed on the server.

**Caution: Record the trial license expiration date**
The system does not notify you when the 60-day trial period license is close to expiration. Record the expiration date of the trial license to prevent any interruption to call services.

Follow these three steps to activate your purchased license(s):

1. **Record the Serial Number of the Server**
2. **Obtain a License Activation Key Code**
3. **Activate the System License**

**Record the Serial Number of the Server**
To request an activation key code for your license, you must know the serial number of the RealPresence Access Director, Appliance Edition server and the license number from your License Certificate.

**To view the serial number and other license information:**

1. Log into the RealPresence Access Director system user interface as a system administrator.
2. Go to Maintenance > License.

The following information displays:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Licensed Calls</td>
<td>Maximum number of calls that the license permits.</td>
</tr>
<tr>
<td>High Availability</td>
<td>Indicates whether the license includes access to High Availability features.</td>
</tr>
<tr>
<td>Remaining trial period</td>
<td>Displays if you are using a trial license and specifies the time remaining in the trial period. Commercial licenses have no trial period limitation.</td>
</tr>
<tr>
<td><strong>Activation Keys</strong></td>
<td></td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number of the RealPresence Access Director system server</td>
</tr>
</tbody>
</table>
To request an activation key code for a new installation:

1. Open a web browser and go to http://support.polycom.com.
2. Select Licensing & Product Registration > Activation/Upgrade.
3. Select All other Polycom Products.
4. Log in or Register for An Account.
5. Click SITE & Single Activation/Upgrade.
6. Accept the EXPORT RESTRICTION agreement.
7. In Product Activation, enter the serial number of your RealPresence Access Director, Appliance Edition server and click Next.
8. Enter the license number from the License Certificate you received for your system and click Activate.
9. Record the Key Code that displays.
10. Click the Upgrade tab to view any Upgrade Key Codes available for your serial number.
11. If an Upgrade Key Code is available, record the key code and use it to activate your new license from the RealPresence Access Director, Appliance Edition user interface. See Activate the System License.
12. If no Upgrade Key Codes are available for your serial number, use the key code you recorded before clicking the Upgrade tab.
To request an activation key code for a major or minor software upgrade:

1. Open a web browser and go to http://support.polycom.com.
2. In the Licensing & Product Registration section, select Activation/Upgrade.
3. Select All Other Polycom Products.
4. Log in or Register for An Account.
5. Click SITE & Single Activation/Upgrade.
6. Accept the EXPORT RESTRICTION agreement.
7. In Product Activation, enter the serial number of your RealPresence Access Director system server and click Next.
8. Click the Upgrade tab to view the Upgrade Key Codes available for your serial number.
9. Record the Upgrade Key Code for the software upgrade and use it to activate your system after installing the upgrade file. See Activate the System License.

Activate the System License

After you obtain an activation key code for your license, you must activate the license in the RealPresence Access Director system, Appliance Edition, user interface.

To activate a license:

1. Log into the RealPresence Access Director, Appliance Edition user interface.
2. Go to Maintenance > License.
3. Enter the Activation key for the license and click Update.
   The system restarts.

Virtual Edition Licensing

Virtual Editions of the RealPresence Access Director system require the Polycom® RealPresence® Platform Director™ system to manage licensing. After you install your license in the RealPresence Platform Director system, you can install a new instance or add an existing instance of the RealPresence Access Director system in the RealPresence Platform Director system. The Platform Director system configures a license server IP address and port number to enable communication between the two systems.

Your RealPresence Access Director, Virtual Edition, communicates regularly with the license server to obtain updated license information, including changes to the number of licensed calls, access to features (for example, High Availability), and license status (active or expired). Occasionally, the system may display alerts related to the status of your license. These alerts will display on the Dashboard on the System Alerts pane. See Monitor System Alerts.


Caution: Restart the RealPresence Access Director instance if you change license allocations

If you change license allocations in the RealPresence Platform Director system for an instance of the RealPresence Access Director system, you must restart the RealPresence Access Director instance for the changes to take effect. See the Polycom RealPresence Platform Director System Administrator Guide, available at support.polycom.com.
View License Information

You can view the license information for your system from the RealPresence Access Director system user interface.

To view license information:

» Go to Maintenance > License Server Settings.

The following information displays:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License server address</td>
<td>The IP address of the RealPresence Platform Director system license server that the RealPresence Access Director system, Virtual Edition, communicates with for license information and updates.</td>
</tr>
<tr>
<td>License server port</td>
<td>The port number of the license server.</td>
</tr>
</tbody>
</table>

View License Alerts

The RealPresence Access Director, Virtual Edition, software communicates regularly with the license server to obtain updated license information, including changes to the number of licensed calls, access to features, and license status (that is, active or expired). Occasionally, the system may display alerts related to the status of your license. These alerts will display on the Dashboard on the System Alerts pane. See Monitor System Alerts.

High Availability Licensing

To use High Availability, you must have RealPresence Access Director system licenses that enable use of the feature.

For the RealPresence Access Director, Appliance Edition, each server requires a system license that includes the High Availability feature. For the Virtual Edition, you need a RealPresence Access Director system license for calls and a capability license to enable the High Availability feature. These licenses must be available on the RealPresence Platform Director system that manages licenses for your RealPresence Access Director instances.

Although not required, Polycom highly recommends that you license each system or allocate each virtual instance with the same number of calls. To determine the number of calls to license for each system, consider the total number of calls you must be able to support at any given time. Remember that if a failover occurs, the remaining active server should have enough licensed call capacity to support the calls that failed.

Many call licensing options are possible. The following table includes examples of two different licensing options:

<table>
<thead>
<tr>
<th>Description</th>
<th>Licensing Option A</th>
<th>Licensing Option B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of calls to support</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Number of licensed calls on HA System 1</td>
<td>50</td>
<td>100</td>
</tr>
</tbody>
</table>
In Licensing Option B, each system can accommodate 100 calls but you can balance the load between systems based on your network requirements. Each system might handle 50 percent of its maximum licensed calls, but if a failover occurs, the remaining active system can accommodate 100 percent of the calls you need to support.

If you activate a license for HA in the RealPresence Access Director, Appliance Edition, your system will reboot when you update the license page. After the system restarts and you log in, the High Availability features are available to use.

For the RealPresence Access Director, Virtual Edition, you must restart the RealPresence Access Director instances after you add the High Availability license capability in the RealPresence Platform Director system.

For complete instructions on activating your licenses, see System Licensing in the Polycom RealPresence Access Director System Administrator Guide. For the RealPresence Access Director, Virtual Edition, see the Polycom RealPresence Platform Director System Administrator Guide.

### Configure Network Settings

Some of the network settings for the RealPresence Access Director system are defined when you install and initially configure the system. These settings may be revised at any time. For information on configuring the initial network settings, see the Polycom RealPresence Access Director Getting Started Guide.

The following topics provide detailed information about network settings:

- Network Settings Overview
- Network Interface Configurations
- Configure Static Route Settings

### Network Settings Overview

Always configure network settings based on how you have deployed your RealPresence Access Director system. For more information on different deployment scenarios and the recommended network interface configurations, see Polycom Unified Communications in RealPresence Access Director System Environments. Note that changing any network settings requires a system restart, which terminates all active calls and logs all users out of the system.

<table>
<thead>
<tr>
<th>Description</th>
<th>Licensing Option A</th>
<th>Licensing Option B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of licensed calls on HA System 2</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Total number of calls supported during a failover</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Result</td>
<td>After a failover, the remaining active system can support a maximum of 50 calls. Any additional calls will fail.</td>
<td>After a failover, the remaining active system can support a maximum of 100 calls.</td>
</tr>
</tbody>
</table>
### Caution: Changing network settings may require a new CA certificate for your system

You must create a certificate signing request to apply for a new CA-signed identity certificate for the RealPresence Access Director system if one or both of the following situations is true:
- You change the host name of the system
- You revise the signaling relay address and some registered or guest endpoints use an IP address instead of an FQDN to establish a TLS connection to the RealPresence Access Director system.

The following table describes all network configuration settings for the RealPresence Access Director system. Fields marked with an asterisk (*) are mandatory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>* Hostname</td>
<td>Hostname of the RealPresence Access Director system. Hostname must begin with a letter and contain only letters, numbers, and internal hyphens. The reserved values appserv* and dmamgk-* cannot be used for host names.</td>
</tr>
<tr>
<td>* Primary DNS</td>
<td>IP address of the primary Domain Name Server (DNS) for the network to which the system connects.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>IP address of the secondary DNS server for the network to which the system connects.</td>
</tr>
<tr>
<td>Tertiary DNS</td>
<td>IP address of the tertiary DNS server for the network to which the system connects.</td>
</tr>
<tr>
<td>Search Domain</td>
<td>One or more domain names, separated by spaces. The system domain from the Domain field is added automatically.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain to which the RealPresence Access Director system belongs. &lt;Host Name&gt;.&lt;Domain&gt;</td>
</tr>
<tr>
<td><strong>Advanced Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Mode of the network interface card.</td>
</tr>
<tr>
<td>Device</td>
<td>MAC address and name of the network interface card.</td>
</tr>
<tr>
<td>* IPv4 Address</td>
<td>IPv4 address of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>* IPv4 Subnet Mask</td>
<td>IPv4 subnet mask of the RealPresence Access Director system’s IP address.</td>
</tr>
<tr>
<td>* IPv4 Default Gateway</td>
<td>IP address of the gateway server used to route network traffic outside the subnet.</td>
</tr>
<tr>
<td><strong>Service Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>SIP/H.323 Settings</strong></td>
<td></td>
</tr>
<tr>
<td>* External SIP/H.323</td>
<td>IP address of the network interface used for SIP and H.323 signaling traffic between the RealPresence Access Director system and external networks.</td>
</tr>
<tr>
<td>Signaling IP</td>
<td></td>
</tr>
<tr>
<td>* Internal SIP/H.323</td>
<td>IP address of the network interface used for internal SIP and H.323 signaling traffic.</td>
</tr>
<tr>
<td>Signaling IP</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Media Relay</strong></td>
<td></td>
</tr>
<tr>
<td>* External Relay IP</td>
<td>IP address of the network interface used for media relay between the RealPresence Access Director system and external networks.</td>
</tr>
<tr>
<td>* Internal Relay IP</td>
<td>IP address of the network interface used for media relay between the RealPresence Access Director system and the internal enterprise network.</td>
</tr>
<tr>
<td><strong>Management IP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>* Management IP</td>
<td>IP address of the network interface used for management traffic, including web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.</td>
</tr>
<tr>
<td><strong>Access Proxy Settings</strong></td>
<td></td>
</tr>
<tr>
<td>* External Access Proxy IP</td>
<td>IP address of the network interface used for access proxy traffic between the RealPresence Access Director system and external endpoints.</td>
</tr>
<tr>
<td>* Internal Access Proxy IP</td>
<td>IP address of the network interface used for access proxy traffic between the RealPresence Access Director system and internal network application servers.</td>
</tr>
<tr>
<td><strong>NAT Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Deployed behind Outside Firewall with NAT | When selected, enables NAT settings for the system.  
* If your system is deployed behind a firewall that translates network IP addresses, you must select this option.  
Disabling this option is possible only if the system is deployed behind an outside firewall without NAT. |
| * Signaling Relay Address   | Required if Deployed behind Outside Firewall with NAT is enabled.  
The RealPresence Access Director system's public IP address for signaling and access proxy traffic. This IP address must be mapped on the outside firewall.  
**Note:** If you change the signaling relay address, you must create and install a new CA certificate on the RealPresence Access Director system if the external endpoint uses IP addresses instead of FQDNs to establish TLS connections to the system. |
| * Media Relay Address       | Required if Deployed behind Outside Firewall with NAT is enabled.  
The RealPresence Access Director system’s public IP address for media traffic. This IP address must be mapped on the outside firewall. |
| **Static Route Settings**   |                                                                                                                                              |
| Available NICs              | Network interfaces selected in the Service network setting tab.                                                                           |
| Selected NICs               | NICs selected from the Available NICs list. Static routes can be configured for the selected NICs.                                        |
| * Network destination       | IP address of the network to which traffic is forwarded.                                                                                   |
| * Netmask                   | Subnet mask of the network destination.                                                                                                     |
Network Interface Configurations

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

If you use more than one network interface in your RealPresence Access Director system, you can configure each network interface for the type of service, or traffic, it communicates. You can distribute the services in various ways based on whether you deploy a standard DMZ configuration or a LAN-WAN configuration.

Using virtual environment tools to add network interfaces after initial installation

If you configure additional network interfaces after you initially install an instance of the RealPresence Access Director system, Virtual Edition, Polycom recommends that you configure the network interfaces from the RealPresence Access Director web user interface. However, if you use your virtual environment tools to add network interfaces, you must reboot the instance to ensure the additional network interfaces display in Admin > Network Settings.

Recommended Configurations for Network Interfaces in a Standard Configuration

<table>
<thead>
<tr>
<th>Number of NICs</th>
<th>Name of Interface</th>
<th>Assigned Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth0</td>
<td>Management, External SIP/H.323 signaling and access proxy, External media, Internal SIP/H.323 signaling and access proxy, Internal media</td>
</tr>
</tbody>
</table>
LAN-WAN Configuration

In a LAN-WAN configuration with 2–4 configured NICs, all network interface IP addresses must be assigned to a WAN-side subnet or a LAN-side subnet. All network interfaces assigned to external, WAN-side services must have IP addresses in the WAN-side subnet. All network interfaces assigned to route traffic to and from the enterprise LAN must have IP addresses in the LAN-side subnet.

In the LAN-WAN configuration, external signaling and access proxy must be assigned to the WAN-side subnet. Internal signaling and access proxy must be assigned to the LAN-side subnet.

The following table lists the recommended network interface settings for the different communication services in a LAN-WAN configuration, based on the number of network interfaces you use.

Recommended Configurations for Network Interfaces in a LAN-WAN Configuration

<table>
<thead>
<tr>
<th>Number of NICs</th>
<th>Name of Interface</th>
<th>Assigned Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>eth0</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal media</td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal media</td>
</tr>
<tr>
<td>4</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>Internal media</td>
</tr>
<tr>
<td></td>
<td>eth3</td>
<td>Management</td>
</tr>
</tbody>
</table>

Polycom, Inc. 37
Configure Network Interfaces
Configure your network interface settings based on your deployment configuration.

To configure network interfaces:

1. Go to Admin > Network Settings > Configure Network Setting.
2. In the Step 1 of 3: General Network Settings window, confirm or reconfigure the general network settings for eth0 as described in Network Settings Overview and click Next.
3. In the Step 2 of 3: Advanced Network Settings window, click each of the network interfaces to configure and complete the following fields as described in Network Settings Overview.
   - IPv4 Address
   - IPv4 Subnet Mask
   - IPv4 Default Gateway: The RealPresence Access Director system uses Linux policy routing; therefore, you must specify a default gateway for each network interface you configure.
4. Click Next.
5. In the Step 3 of 3: Service Network Settings window, select the IP address of the network interface to assign to each type of traffic, as shown in the following table (see Standard Configuration or LAN-WAN Configuration for recommended settings):

<table>
<thead>
<tr>
<th>Settings</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP/H.323</td>
<td>• External SIP/H.323 Signaling IP</td>
</tr>
<tr>
<td></td>
<td>• Internal SIP/H.323 Signaling IP</td>
</tr>
<tr>
<td>Media Relay</td>
<td>• External Media Relay IP</td>
</tr>
<tr>
<td></td>
<td>• Internal Media Relay IP</td>
</tr>
</tbody>
</table>

Recommended Configurations for Network Interfaces in a LAN-WAN Configuration

<table>
<thead>
<tr>
<th>Number of NICs</th>
<th>Name of Interface</th>
<th>Assigned Traffic</th>
</tr>
</thead>
</table>
| 3              | eth0              | External SIP/H.323 signaling and access proxy  
|                |                   | External media                      |
|                | eth1              | Internal SIP/H.323 signaling and access proxy 
|                |                   | Internal media                      |
|                | eth2              | Management                          |
| 4              | eth0              | External SIP/H.323 signaling and access proxy |
|                | eth1              | External media                      |
|                | eth2              | Internal media                      |
|                | eth3              | Internal SIP/H.323 signaling and access proxy  
|                |                   | Management                          |
Configure Static Route Settings

Depending on how you have deployed the RealPresence Access Director system in your network, different routing policies may be applicable for different traffic destinations. Asymmetric routing issues may occur if the RealPresence Access Director system is directly connected to multiple subnets. In this case, you must define static routes for routing traffic to the correct network destination.

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

To add a static route for a network interface:

1. Go to Admin > Static route setting.
2. From the list of Available NICs, select the network interface for the new static route.
3. Click the right arrow to add the network interface to the list of Selected NICs.
4. Enter the Static route setting information:
   - Network destination: The IP address of the network to which traffic is forwarded. For example, the IP address of the enterprise intranet.
   - Netmask: The subnet of the network destination.

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

Caution: Changing network settings may require a new CA certificate for your system

You must create a certificate signing request to apply for a new CA-provided identity certificate for the RealPresence Access Director system if one or both of the following situations is true:

- You change the host name of the system
- You revise the signaling relay address and some registered or guest endpoints use an IP address instead of an FQDN to establish a TLS connection to the RealPresence Access Director system.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP</td>
<td>Management IP</td>
</tr>
<tr>
<td>Access Proxy</td>
<td>• External Access Proxy IP</td>
</tr>
<tr>
<td></td>
<td>▶ If the appropriate IP address does not already display in this field, select it from the Available IP address list, then click the right arrow to move the IP address to the External Access Proxy IP list.</td>
</tr>
<tr>
<td></td>
<td>• Internal Access Proxy IP</td>
</tr>
<tr>
<td></td>
<td>▶ Note: Only one interface can be assigned as the internal access proxy IP address.</td>
</tr>
<tr>
<td>NAT</td>
<td>If your system is deployed behind a firewall that translates network IP addresses, select Deployed behind Outside Firewall with NAT and complete these fields:</td>
</tr>
<tr>
<td></td>
<td>• Signaling relay address</td>
</tr>
<tr>
<td></td>
<td>• Media relay address</td>
</tr>
</tbody>
</table>
Gateway: The gateway through which traffic can reach the network destination. The gateway must be in the same subnet with the selected NIC.

5. Click **Add**.
   The new static route for the network interface displays in the **Static Route list**.

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

To delete a static route for a network interface:

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

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

To remove a network interface from the **Selected NICs list**:

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

Configure Two-System Tunnel Settings (Optional)

You can deploy two RealPresence Access Director systems in a tunnel configuration. In this model, one system is deployed as the tunnel server in the corporate DMZ and the other system is deployed as the tunnel client inside your enterprise network. All traffic to and from the Internet flows through the tunnel server, and all traffic to and from the enterprise network flows through the tunnel client. Communication between the tunnel server and tunnel client traverses the enterprise firewall inside the tunnel. The exception is management traffic. Each system has a management network interface so management traffic does not traverse the tunnel.

Note: Two-system tunnel deployment requires two licenses

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

If you deploy two RealPresence Access Director, Appliance Edition systems, activate the license for each server before enabling the two-system tunnel. See **System Licensing**.

In a tunnel configuration, port mapping on the firewall between the tunnel server and the tunnel client is not required. Instead, when you enable the tunnel feature on the tunnel server, the tunnel port automatically listens for communication from the tunnel client. When you enable the tunnel feature on the tunnel client, the client then registers to the tunnel server through the listening tunnel port.

During the registration process, the tunnel server detects the IP address of the tunnel client. Additionally, the tunnel client sends the internal signaling and media IP address to the tunnel server. The tunnel client uses this IP address to communicate with the internal RealPresence DMA system. After the tunnel client
registration is complete, the tunnel server establishes a secure tunnel connection and stops listening on the
tunnel port.

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

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

The tunnel connection between the two systems uses a self-signed certificate that is dedicated for tunnel
use.

**Compatibility with an HTTP tunnel proxy**

If you deploy two systems in a tunnel configuration, the HTTP tunnel proxy feature within access proxy is not supported. If you configure an HTTP tunnel proxy before you enable the two-system tunnel, the option to enable the two-system tunnel is not available.

**Compatibility with TURN services**

If you deploy two systems in a tunnel configuration, the TURN server feature is not supported. If you enable the TURN server on either of the single RealPresence Access Director systems before you set up a two-system tunnel, you must disable the TURN server before you enable the tunnel feature.

**Configure Network and Tunnel Settings**

The following topics describe how to configure the network settings and the tunnel server and tunnel client
settings for the tunnel:

- Configure Network Settings on the Tunnel Server
- Configure Network Settings on the Tunnel Client
- Configure Two-box Tunnel Settings on the Tunnel Server
- Configure Two-box Tunnel Settings on the Tunnel Client

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

**Configure Network Settings on the Tunnel Server**

You can configure network settings for the tunnel server for one to four network interfaces.

**To configure network settings for the tunnel server:**

1. From your web browser, enter the IP address of the RealPresence Access Director system that will
act as the tunnel server and log into the user interface.
2. Go to Admin > Network Settings > Configure Network Setting.
3. In the Step 1 of 3: General Network Settings window, confirm the general network settings for
eth0 as described in Network Settings Overview and click Next.
4 In the Step 2 of 3: Advanced Network Settings window, click each of the network interfaces to configure and complete the following fields as described in Network Settings Overview.

- IPv4 Address
- IPv4 Subnet Mask
- IPv4 Default Gateway

5 Click Next.

6 In the Step 3 of 3: Service Network Settings window, select the IP address of the network interface to assign for each type of traffic and for communication between the tunnel server and tunnel client:

- External Signaling IP—The IP address of the network interface used for SIP and H.323 signaling traffic between the RealPresence Access Director system and external networks.
- External Relay IP—The IP address of the network interface used for media relay between the RealPresence Access Director system and external networks.
- Management IP—The IP address of the network interface used for management traffic, including web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.
  ♦ If you use three or four network interfaces on the tunnel server, you can assign different network interfaces for tunnel communication traffic between the two systems and for management traffic. In this case, select the network interface used for management traffic in the Management IP field. Configure the interface for tunnel communication between the two systems in the Two-box Tunnel Settings screen (see Configure Two-box Tunnel Settings on the Tunnel Server).
- External Access Proxy IP: If the appropriate IP address does not already display in this field, select it from the Available IP address list, then click the right arrow to move the IP address to the External Access Proxy IP list.

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

- Signaling relay address: The RealPresence Access Director system’s public IP address for signaling traffic. This IP address must be mapped on the outside firewall.
- Media relay address: The RealPresence Access Director system’s public IP address for media traffic. This IP address must be mapped on the outside firewall.
  Depending on your network interface configuration, the signaling relay address and the media relay address may be the same IP address.

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

Configure Network Settings on the Tunnel Client

You can configure network settings for the tunnel client for one to three network interfaces.

To configure network settings for the tunnel client:

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

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

3 In the Step 1 of 3: General Network Settings window, confirm the general network settings for eth0 as described in Network Settings Overview and click Next.
  The General Network Settings that display are the settings configured for eth0 during installation and initial configuration.
4. In the **Step 2 of 3: Advanced Network Settings** window, click each of the network interfaces to configure and complete the following fields as described in **Network Settings Overview**.

- IPv4 Address
- IPv4 Subnet Mask
- IPv4 Default Gateway

5. Click **Next**.

6. In the **Step 3 of 3: Service Network Settings** window, select the network interface to assign as the **Management IP** address.

   The network interface that handles management traffic is based on the number of network interfaces configured on the tunnel client. See **Network Interface Configurations** in *Polycom Unified Communications in RealPresence Access Director System Environments*.

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

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

**Configure Two-box Tunnel Settings on the Tunnel Server**

If your license supports tunnel encryption, you must synchronize the time on the tunnel server and the tunnel client to the same Network Time Protocol (NTP) server before encrypting the tunnel. See **Configure Time Settings**.

**Note: Tunnel encryption not available for some installations**

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

**To configure settings on the tunnel server:**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Tunnel</td>
<td>Select to enable the two-system tunnel feature.</td>
</tr>
</tbody>
</table>

**Settings**

<table>
<thead>
<tr>
<th>Server</th>
<th>Select <strong>Server</strong> to enable the system to operate as a tunnel server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td></td>
</tr>
</tbody>
</table>
To configure two-box tunnel settings on the tunnel client:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Tunnel</td>
<td>The tunnel feature is enabled if you have configured the tunnel server.</td>
</tr>
</tbody>
</table>

Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Select Client to enable the system to operate as the tunnel client.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
</tr>
</tbody>
</table>
Configure Access Proxy Settings

The access proxy feature in the RealPresence Access Director system provides reverse proxy services for external devices. You can configure access proxy settings to enable firewall/NAT traversal for login, registration, and call requests. When the RealPresence Access Director system receives a request from a remote user, the system accepts or denies the request, based on your basic Access Control List (ACL) settings (see Configure Basic Access Control List Settings.) If the request is accepted, the RealPresence Access Director system sends a new request on behalf of the remote user to the appropriate application server.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted tunnel</td>
<td>When selected, communications between the tunnel server and tunnel client are encrypted. <strong>Note:</strong> This option displays only if you purchase a license that supports encryption of the tunnel between two systems. Select this option to encrypt the tunnel communications. <strong>This setting must be the same on both the tunnel server and tunnel client.</strong></td>
</tr>
<tr>
<td>Performance profile</td>
<td>If you enable tunnel encryption, select a performance profile. <strong>Premium:</strong> 10 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 600M  <strong>Regular:</strong> 6 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 400M  <strong>Base:</strong> 2 CPU core are allocated to tunnel processes. Maximum tunnel throughput: 200M  <strong>The profiles on the tunnel server and client must match.</strong></td>
</tr>
<tr>
<td>* Local tunnel client address</td>
<td>The IP address and port number of the tunnel client. Default port: 1194 <strong>Note:</strong> Polycom recommends that you use the default port number 1194, but you can use any value from 1190–1199 or 65380–65389.</td>
</tr>
<tr>
<td>* Remote tunnel server address</td>
<td>The IP address and port number of the tunnel server. Default port: 1194</td>
</tr>
<tr>
<td>* Internal signaling/media/access proxy IP of tunnel client</td>
<td>The IP address of the network interface that the tunnel client uses for internal signaling, internal media, and internal access proxy communication with the RealPresence DMA system.</td>
</tr>
</tbody>
</table>

3 Click **Update**. The system restarts.

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

The access proxy feature in the RealPresence Access Director system provides reverse proxy services for external devices. You can configure access proxy settings to enable firewall/NAT traversal for login, registration, and call requests. When the RealPresence Access Director system receives a request from a remote user, the system accepts or denies the request, based on your basic Access Control List (ACL) settings (see Configure Basic Access Control List Settings.) If the request is accepted, the RealPresence Access Director system sends a new request on behalf of the remote user to the appropriate application server.

The RealPresence Access Director system is configured with three default reverse proxies that route communication requests based on the type of target application server:
- **HTTPS_proxy**—HTTPS servers that provide management services (RealPresence Resource Manager system, Polycom® RealPresence® ContentConnect™ system), and web-based video conferencing services (RealPresence Web Suite)
- **LDAP_proxy**—LDAP servers that provide directory services
- **XMPP_proxy**—XMPP servers that provide message, presence, or other XMPP services

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

- **PassThrough_proxy**—A passthrough reverse proxy configuration provides transparent relay of communication requests through the RealPresence Access Director system to internal application servers. PassThrough_proxy is used primarily for backward compatibility with the TCP reverse proxy feature. Note that if you upgrade your system to a new version, PassThrough_proxy will not display on the main Access Proxy Settings page if you did not configure a TCP reverse proxy in a previous version of the RealPresence Access Director system.

- **HTTP tunnel proxy**—An HTTP tunnel proxy enables SIP guest users to attend web-based video conferences hosted by an enterprise’s RealPresence Web Suite. Due to restrictive firewall rules, if a SIP guest client cannot establish a native SIP/RTP connection to a Web Suite video conference, the RealPresence Access Director system can act as a web proxy to tunnel the SIP call on port 443. Once the SIP guest client is connected to a meeting, the RealPresence Access Director system continues to tunnel TCP traffic, including SIP signaling, media, and Binary Floor Control Protocol (BFCP) content.

  **Note: HTTP tunnel proxy configuration remains after upgrading**
  If you created an HTTP tunnel proxy in a previous version of the RealPresence Access Director system, the HTTP tunnel proxy configuration will display on the Access Proxy Settings page after you upgrade your system to a new version.

The default proxies may be edited or you can add new proxies for various internal application servers. When you configure the proxies, you must specify an external IP address and an external listening port for access proxy. Based on the network settings you configured (see **Network Interface Configurations**), you may have external access proxy services assigned to more than one network interface. You can reuse an external IP address but the port, in most cases, must be unique for each proxy configuration that uses the same external IP address. For example, if you create two proxy configurations for LDAP directory services, the combined external IP address for access proxy and the external listening port cannot be the same for both LDAP proxy configurations.

If you create an HTTP tunnel proxy, both the HTTP tunnel proxy and the default **HTTPS_proxy** can use port 443 on the same external access proxy IP address.

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

**Example 1**

<table>
<thead>
<tr>
<th>Name of Proxy</th>
<th>External IP Address for Access Proxy</th>
<th>External Listening Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_proxy_1</td>
<td>172.20.102.58</td>
<td>389</td>
</tr>
<tr>
<td>LDAP_proxy_2</td>
<td>172.20.102.58</td>
<td>9980</td>
</tr>
<tr>
<td>HTTPS_proxy</td>
<td>172.20.102.58</td>
<td>443</td>
</tr>
<tr>
<td>HTTP tunnel proxy</td>
<td>172.20.102.58</td>
<td>443</td>
</tr>
</tbody>
</table>
Example 2

<table>
<thead>
<tr>
<th>Name of Proxy</th>
<th>External IP Address for Access Proxy</th>
<th>External Listening Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP_proxy_1</td>
<td>172.20.102.58</td>
<td>389</td>
</tr>
<tr>
<td>LDAP_proxy_2</td>
<td>172.20.102.60</td>
<td>389</td>
</tr>
</tbody>
</table>

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

![Caution: Configure network setting before access proxy settings]

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

Add a New Proxy Configuration

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

To add a new proxy configuration:

1. Go to Configuration > Access Proxy Settings.
2. Under Actions, click Add.
3. In the Step 1 of 2: Protocol Selection window, select the Protocol for the new proxy and click Next.
4. In the Step 2 of 2: Detailed Settings window, configure the settings for the specific protocol of the proxy, as described in the following sections:
   - Configure HTTPS Proxy Settings
   - Configure LDAP Proxy Settings
   - Configure XMPP Proxy Settings
   - Configure a Passthrough Proxy
   - Configure HTTP Tunnel Settings

Configure HTTPS Proxy Settings

The access proxy feature enables external users to access different internal HTTPS servers. The RealPresence Access Director system accepts a request from a remote user, then sends a new request on behalf of the user to the correct application server based on the HTTPS reverse proxy settings you configure.

When the RealPresence Access Director system is integrated with a Polycom RealPresence Resource Manager system, access proxy enables remote endpoints to be provisioned and managed by the RealPresence Resource Manager system. When the RealPresence Access Director system receives a login and provisioning request from an external endpoint, it sends the request to the HTTPS provisioning server configured within the RealPresence Resource Manager system.
When you configure the HTTPS Proxy settings, you can add multiple HTTPS next hops. For each next hop, you must apply a filter that's based on the HTTPS request message header received from the endpoint. The RealPresence Access Director system uses the filter and other settings to send the connection request to the correct internal HTTPS application server. Two filters are available:

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

**Caution: Include FQDNs as SANs in certificate signing request**

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

To configure HTTPS proxy settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this HTTPS proxy configuration</td>
</tr>
<tr>
<td>External IP address</td>
<td>The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.</td>
</tr>
</tbody>
</table>
| External listening port       | The external port at which the RealPresence Access Director system listens for HTTPS proxy traffic. Default port: 443 Port range: 9980–9999  
**Note:** The RealPresence Access Director system automatically redirects inbound access proxy traffic on ports 443 and 389 to the internal ports 65100–65130 reserved on the system's loopback interface private IP address. The CentOS operating system does not allow processes without root ownership to listen on ports <1024. Redirecting access proxy traffic on ports <1024 to the internal ports 65100–65130 enables the access proxy process to function correctly. |
| Internal IP address           | The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards HTTPS requests from this IP address to the requested application server.                                                                                                                                                                                                 |
To add the Next hops. See To add a next hop based on the Request-URI filter: and To add a next hop based on the Host header filter:.

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

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify certificate from internal server</td>
<td>When selected, access proxy verifies the certificate from the internal HTTPS server (the RealPresence Resource Manager system, the Polycom ContentConnect system, or the RealPresence Web Suite).</td>
</tr>
</tbody>
</table>

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

To add a next hop based on the Host header filter:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Request-URI</td>
</tr>
<tr>
<td>Name</td>
<td>The unique name of this next hop</td>
</tr>
<tr>
<td>System</td>
<td>Polycom Management System or Polycom Content Sharing Suite (also called Polycom ContentConnect)</td>
</tr>
<tr>
<td></td>
<td>Note: Add a separate Request-URI next hop if you need to configure HTTPS settings for both systems.</td>
</tr>
<tr>
<td>Address</td>
<td>The internal IP address of the target HTTPS server. After accepting the HTTPS request from the external endpoint, the RealPresence Access Director system sends a new HTTPS request to this IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The listening port of the internal HTTPS server.</td>
</tr>
</tbody>
</table>

3. Click OK to save the configuration.
4. Repeat the steps to add other next hops as needed.
To prioritize next hops:

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

To edit an HTTPS next hop:

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

To delete an HTTPS next hop:

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

Configure LDAP Proxy Settings

LDAP reverse proxy configurations can be added to access different LDAP directory servers, such as the RealPresence Resource Manager system LDAP server or an Active Directory server. If you configure a new LDAP proxy with the same external IP address as the system’s default LDAP_proxy, you must assign a port other than 389 to one of the proxies. The following instructions list the alternate port range.

To configure LDAP proxy settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The internal IP address of the target HTTPS server, such as the RealPresence Web Suite. After accepting the HTTPS request from the external endpoint, the RealPresence Access Director system sends a new HTTPS request to this IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>The listening port of the internal application server.</td>
</tr>
</tbody>
</table>
Configure XMPP Proxy Settings

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

To configure XMPP proxy settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this LDAP proxy configuration</td>
</tr>
<tr>
<td>External IP address</td>
<td>The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.</td>
</tr>
<tr>
<td>External listening port</td>
<td>The external port at which the RealPresence Access Director system listens for LDAP traffic. Default port: 389 Port range: 9980–9999 Note: The RealPresence Access Director system automatically redirects inbound access proxy traffic on ports 443 and 389 to the internal ports 65100–65130 reserved on the system's loopback interface private IP address. The CentOS operating system does not allow processes without root ownership to listen on ports &lt;1024. Redirecting access proxy traffic on ports &lt;1024 to the internal ports 65100–65130 enables the access proxy process to function correctly.</td>
</tr>
<tr>
<td>Internal IP address</td>
<td>The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards LDAP requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The internal IP address of the target LDAP server. The RealPresence Access Director system sends a new request to the next hop IP address on behalf of the external user.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port at which the internal LDAP application server listens. Default LDAP port: 389</td>
</tr>
<tr>
<td>Require client certificate from the remote endpoint</td>
<td>When selected, access proxy requests and verifies the client certificate from the remote endpoint.</td>
</tr>
<tr>
<td>Verify certificate from internal server</td>
<td>When selected, access proxy verifies the certificate from the internal LDAP server.</td>
</tr>
</tbody>
</table>

5. Click Done, and then click OK to confirm the configuration settings and restart access proxy.
Configure a Passthrough Proxy

A passthrough reverse proxy configuration provides transparent relay of communication requests through the RealPresence Access Director system to internal application servers. Passthrough reverse proxy is used primarily for backward compatibility with the TCP reverse proxy feature and appears on the main Access Proxy Settings page after upgrading the system software only if you configured a TCP reverse proxy in a previous version of the RealPresence Access Director system.

Connections to a RealPresence Web Suite Experience Portal or Services Portal should not be configured as a passthrough proxy. Instead, these connections should be configured as next hops based on the host header filter within the default HTTPS_proxy or in a new HTTPS reverse proxy configuration. See To configure HTTPS proxy settings.

5 Click Done, and then click OK to confirm the configuration settings and restart access proxy.
To configure passthrough reverse proxy settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of this passthrough proxy configuration</td>
</tr>
<tr>
<td>External IP address</td>
<td>The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.</td>
</tr>
<tr>
<td>External listening port</td>
<td>The external port at which the RealPresence Access Director system listens for passthrough traffic.  Port range: 8080, 443, 9980–9999</td>
</tr>
<tr>
<td>Internal IP address</td>
<td>The internal access proxy IP address of the RealPresence Access Director system (specified when you configure network settings). The system forwards passthrough requests from this IP address to the requested application server.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>The internal IP address of the target application server. The RealPresence Access Director system sends a new request to the next hop IP address on behalf of the external user.</td>
</tr>
<tr>
<td>Next hop port</td>
<td>The port at which the internal application server listens.</td>
</tr>
</tbody>
</table>

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

Configure HTTP Tunnel Settings

An HTTP tunnel enables SIP guest users to attend video conferences hosted by the RealPresence Web Suite. Some restrictive networks block outgoing UDP-based traffic and can limit outgoing TCP traffic to ports 80 and 443. In these situations, if a SIP guest client cannot establish a native SIP/RTP connection to a RealPresence Web Suite video conference, the RealPresence Access Director system can act as a web proxy to tunnel the SIP guest call on port 443. Once the SIP client is connected to a meeting, the RealPresence Access Director system continues to tunnel TCP traffic, including SIP signaling, media, and BFCP content.

The HTTP tunnel proxy uses auto-discovery to ensure that a RealPresence Web Suite SIP guest call is routed through the HTTP tunnel proxy when necessary. When a RealPresence Web Suite SIP guest user attempts to join a meeting, auto-discovery determines if standard SIP and media ports are available for the call. If not, the call is routed through the HTTP tunnel proxy.
You can configure both the default HTTPS_proxy and an HTTP tunnel proxy to use the same external IP address and standard port 443. If you configure a port other than 443 as the external listening port for HTTP tunnel proxy calls, these calls may fail if the network from which the SIP guest client calls blocks outgoing traffic to other ports.

The following conditions apply to the HTTP tunnel proxy:

- Only one HTTP tunnel proxy can be configured.
- The HTTP tunnel proxy does not support SVC video conferencing.
- The RealPresence Access Director system supports a maximum of 50 concurrent HTTP tunnel calls. After a call ends, the system recycles the port allocation.
- Use of an HTTP tunnel proxy is not supported with two RealPresence Access Director systems deployed in a tunnel configuration.

Before you configure an HTTP tunnel proxy, complete the steps in each of these sections:

- Assign external access proxy IP addresses in network settings
  See Access Proxy Settings
- Configure the HTTPS proxy settings
  See Configure HTTPS Proxy Settings
- Configure the Web Suite Services Portal (or Experience Portal) as a next hop in HTTPS proxy settings
  See To add a next hop based on the Host header filter:

To configure HTTP tunnel proxy settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the HTTP tunnel proxy configuration</td>
</tr>
<tr>
<td>External IP address</td>
<td>The external IP address of the RealPresence Access Director system network interface that receives access proxy traffic.</td>
</tr>
<tr>
<td>External listening port</td>
<td>The external port at which the RealPresence Access Director system listens for HTTP tunnel requests. Recommended HTTP tunnel port: 443 Range: 80, 9980–9999</td>
</tr>
</tbody>
</table>

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

Edit Proxy Settings
You can revise the settings of a proxy configuration as needed.
To edit proxy settings:

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

Delete Proxy Configurations

Delete a proxy configuration if it is no longer in use.

To delete a proxy configuration:

1. Go to Configuration > Access Proxy Settings.
2. Select the proxy to delete.
3. Under Actions, click Delete.
4. Click OK to confirm the deletion.

Configure Basic Access Control List Settings

Basic Access Control List (ACL) settings provide simple-to-use control over inbound access to your video network through the RealPresence Access Director system. In Basic ACL Settings, you can define the following registration policy and call policy settings to control access to your network:

- Users and devices that are allowed to register to your network call server through the RealPresence Access Director system
- Devices that are allowed to call into your network through the RealPresence Access Director system
- Destinations inside your network that are accessible from callers outside of your network

When you install a new RealPresence Access Director system, the following Basic ACL Settings are enabled by default:

- Enable Registration Policy
- Allow registration from provisioned devices
- Enable Call Policy
- Allow call from registered devices

Caution: You must configure access proxy settings to enable device registration and provisioning

When you configure Basic ACL Settings, you must specify the login, registration, or call requests to allow. If not specifically allowed, the system will deny requests. To ensure that the default settings function as intended, be sure to configure your access proxy settings to enable endpoints to register and be provisioned (see Configure HTTPS Proxy Settings).
How Basic ACLs Work

An ACL rule defines the specific conditions of registration requests or call signaling traffic. A setting is the action that the RealPresence Access Director system will take when the conditions of the rule are matched (allow or deny). Basic ACL settings require you to enter minimal information about the allowed registrations and calls to your network. Based on your input, the RealPresence Access Director system then automatically creates the necessary ACL rules and settings on the appropriate SIP and H.323 ports that allow or deny access to your network. The basic ACL settings you configure are also applied to any new external SIP ports you add to your system.

**Note: Configuring Basic ACL Settings during active registrations or calls**
You can initially configure or revise Basic ACL Settings without interrupting any active registrations, logins, and calls.

Due to their ease of use, Polycom recommends that you use basic ACL settings to control access to your video conferencing network. However, you can configure Advanced ACL Settings to create specific customized ACL rules, conditions, variables, and settings, for your network. See Define Advanced Access Control List Rules for detailed instructions. Note that rules the RealPresence Access Director system automatically creates based on your basic ACL settings are labeled **Basic**. The default system rules and any custom rules that you configure are labeled **Advanced**.

You can view ACL log information in the sipService log and the h323Service log (Diagnostics > System Log Files). Additionally, you can view denied registration attempts and denied calls (Diagnostics > Registration History and Diagnostics > Call History).

**Note: Using wildcard values in Basic ACL Settings**
Some basic ACL settings, such as IP addresses or aliases, support use of an asterisk (*) as a wildcard value. For these settings, you can use only one wildcard value per entry. For example, if you enter the IP address 120.*.102.*, the RealPresence Access Director system recognizes only the first wildcard value and interprets the IP address as 120.*. The system will proxy all registration or call requests from devices with IP addresses that begin with 120.

Configure Registration Policy Settings

You can configure specific registration policy settings to limit which registration requests the RealPresence Access Director system proxies to your call server. The following table describes the registration policy settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Registration Policy | When this setting is enabled, you can configure how the RealPresence Access Director system responds when it receives registration requests. Based on the settings you configure, the system allows or denies registration requests to be proxied to your call server.  
**Note:** Both Enable Registration Policy and Allow registration from provisioned devices are enabled by default in new installations of the RealPresence Access Director system. With these two settings enabled, the default action of the RealPresence Access Director system is to deny registration requests except for those that come from provisioned devices. |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Allow registration from provisioned devices | When enabled, the RealPresence Access Director system will proxy registration requests from devices that are dynamically provisioned by the RealPresence Resource Manager system.  
**Note:** Both Enable Registration Policy and Allow registration from provisioned devices are enabled by default in new installations of the RealPresence Access Director system. With these two settings enabled, the default action of the RealPresence Access Director system is to deny registration requests except for those that come from provisioned devices. To configure access to a provisioning server, see Configure HTTPS Proxy Settings. |
| Allow registration from these IP addresses   | When enabled, you can add specific IP addresses or IP address ranges for which the RealPresence Access Director system will proxy registration requests. This may be necessary for some older-model Polycom endpoints that cannot be dynamically managed, or for non-Polycom endpoints.  
The **IP Address** field supports use of one wildcard value (*) per IP address. For example, if you enter 120.*.102.*, the RealPresence Access Director system recognizes only the first wildcard value and interprets the IP address as 120.*. The system will proxy all registration requests from devices with IP addresses that begin with 120.  
**Note:** If you add IP addresses and later disable this setting, the registration rules that the RealPresence Access Director system created are removed from all ports. However, the IP addresses you entered remain in the IP Address list. If you later select this setting again, you do not need to re-enter IP addresses.  
To add an IP address or IP address range, see To allow registration from an IP address:  
To delete an IP address or IP address range, see To delete an allowed IP address: |
| Allow registration with these aliases        | When enabled, you can specify the allowed aliases from which the RealPresence Access Director system will proxy registration requests, regardless of the device IP address.  
You can add aliases using any of the following formats:  
- **SIP:** URI  
- **H.323:** H.323-ID, E.164 ID, H.323-URL, E-mail name  
**Note:** The RealPresence Access Director system creates rules that apply to all SIP and H.323 formats, regardless of the format you enter.  
An alias can contain the following characters:  
a–z  
A–Z  
0–9  
.  
_  
#  
@  
**Note:** An alias can also contain one wildcard value.  
To add an alias, see To allow registration from an alias:  
To delete an alias, see To delete an allowed alias: |
To allow registration from an IP address:

1. Go to Configuration > Basic ACL Settings.
2. Select Enable Registration Policy.
3. Select Allow registration from these IP addresses.
4. In the IP Address field, enter the IP address for which to allow registration, then click Add.
   The IP address displays in the IP Address list.
5. Click Update.

To delete an allowed IP address:

1. Go to Configuration > Basic ACL Settings.
2. In the IP Address list, select the IP address to delete, then click Delete.
   The IP address is removed from the IP Address list.
3. Click Update.

To allow registration from an alias:

1. Go to Configuration > Basic ACL Settings.
2. Select Enable Registration Policy.
3. Select Allow registration with these aliases.
4. In the Alias field, enter the alias for which to allow registration, then click Add.
   The alias displays in the Alias list.
5. Click Update.

To delete an allowed alias:

1. Go to Configuration > Basic ACL Settings.
2. In the Alias list, select the alias to delete, then click Delete.
   The alias is removed from the Alias list.
3. Click Update.
Configure Call Policy Settings

You can configure specific call policy settings to specify which incoming calls to your network are allowed and to which destinations. The RealPresence Access Director system then proxies the allowed calls to your call server based on the settings you configure. The following table describes the call policy settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Call Policy                           | When this setting is enabled, you can configure how the RealPresence Access Director system responds when it receives incoming calls to your video network. Based on the settings you configure, the system allows or denies calls to be proxied to your call server.  
**Note:** Both Enable Call Policy and Allow call from registered devices are enabled by default in new installations of the RealPresence Access Director system. With these two settings enabled, the default action of the RealPresence Access Director system is to deny calls except for those that come from registered devices. |
| Allow call from registered devices           | When enabled, the RealPresence Access Director system will proxy calls from registered devices. By default, the RealPresence Access Director system will proxy all calls from registered devices. However, these calls are subject to RealPresence DMA system dial rules.  
If this setting is disabled, registered users will be subject to the same ACL rules that the RealPresence Access Director system applies to guest users.  
**Note:** Both Enable Call Policy and Allow call from registered devices are enabled by default in new installations of the RealPresence Access Director system. With these two settings enabled, the default action of the RealPresence Access Director system is to deny calls except for those that come from registered devices. |
| Allow call to the following VMR prefixes or ranges | When enabled, the RealPresence Access Director system will proxy calls to destinations that can be reached from the Internet. The system will allow calls as follows:  
• To a call destination with a prefix that matches a prefix you configure here.  
• To a call destination within a range that matches a range you configure here.  
**Note:** You can configure both prefixes and ranges. |
| Prefix                                       | The RealPresence Access Director system will proxy calls to call destinations with a prefix that matches a prefix you add to the prefix and range list. When you add a prefix, the RealPresence Access Director system automatically includes the wildcard character (*) after the prefix.  
**Note:** Dial string prefixes must also be defined in the RealPresence DMA system. |
| Range                                        | The RealPresence Access Director system will proxy calls from the Internet to destinations that are included within any ranges that you configure here.  
**Note:** A VMR range can include the prefixes of the VMR numbers. The RealPresence Access Director system will allow calls only to destinations that exactly match a range that you specify. |
To allow calls to destinations with specific prefixes or ranges:

1. Go to Configuration > Basic ACL Settings and click the Call Policy tab.
2. Select Enable Call Policy, if not already enabled.
3. Select Allow call to the following VMR prefixes or ranges.
4. Complete one or both of the following steps:
   - Select Prefix, enter the prefix value, then click Add.
   - Select Range, enter a range of VMR values, then click Add.
   The prefix and range values display in the list of prefixes and ranges. Note that an asterisk is added after each prefix value to ensure that any all destinations with the prefix can be reached.
5. Click Update.

To delete a prefix or range:

1. Go to Configuration > Basic ACL Settings and click the Call Policy tab.
2. In the list of VMR prefixes and ranges, select the VMR prefix or range to delete, then click Delete.
3. Click Update.

To add customized allowed callers and callees:

1. Go to Configuration > Basic ACL Settings and click the Call Policy tab.

### Setting | Description
--- | ---
Custom allow entries | Custom entries consist of a caller (source) alias and a callee (destination) alias. The RealPresence Access Director system will proxy calls from the caller aliases to the callee aliases that you specify. You can add aliases using any of the following formats:
- SIP: URI
- H.323: H.323-ID, E.164 ID, H.323-URL, E-mail name
**Note:** The RealPresence Access Director system creates rules that apply to all SIP and H.323 formats, regardless of the format you enter.
An alias can contain the following characters:
a–z
A–Z
0–9
- 
_
#
.
@
**Note:** An alias can also contain one wildcard value.

| Caller | A caller alias specifies the source alias of the device making the call. |
| Callee | A callee alias specifies the destination alias of the device receiving the call. |
2 Select **Enable Call Policy**, if not already enabled.
3 Select **Custom allow entries**.
4 In the **Caller** field, enter the alias of an allowed caller.
5 In the **Callee** field, enter the alias of an allowed callee, then click **Add**. The caller and callee combination displays in the custom allow entries list.

**To delete customized allowed callers and callees:**
1 Go to **Configuration > Basic ACL Settings** and click the **Call Policy** tab.
2 In the list of custom allow entries, select the caller and callee combination to delete, then click **Delete**.
3 Click **Update**.

**Manage Certificates**

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

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

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

- **How Certificates Are Used**
- **Accepted Forms of Certificates**
- **Certificate Procedures**
- **View Installed Certificates**
- **View Certificate Details**
- **Add a Certificate Authority’s Public Certificate**
- **Create a Certificate Signing Request**
- **Create a Certificate Signing Request**
- **Review the Signed Certificate**
- **Add the Signed Certificate to the KEY_STORE**
- **Refresh the Server SSL Self-Signed Certificate**
- **Replace a Signed Certificate**
- **Delete a Certificate**
How Certificates Are Used

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

- When you log into the RealPresence Access Director system's user interface from your browser, the RealPresence Access Director system offers an X.509 certificate to identify itself to your browser client.
  - The RealPresence Access Director system’s certificate must have been signed by a certificate authority.
  - The browser must be configured to trust that certificate authority (beyond the scope of this documentation).
- When a client sets up an HTTPS, LDAP, or XMPP connection with access proxy, the RealPresence Access Director system offers an X.509 certificate to identify itself.
- When a client sends SIP messages with TLS transport, the RealPresence Access Director system offers an X.509 certificate to identify itself.
- When the RealPresence Access Director system connects to a RealPresence Resource Manager system, the RealPresence Access Director system may present a certificate to the RealPresence Resource Manager system to identify itself.
- When the RealPresence Access Director system connects to another RealPresence Access Director system or other session border controller (SBC) for a SIP enterprise-to-enterprise call, the RealPresence Access Director system presents its certificate to the other system to identify itself.

Accepted Forms of Certificates

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

<table>
<thead>
<tr>
<th>Encoding</th>
<th>Protocol / File Type</th>
<th>Description and Installation Method</th>
</tr>
</thead>
</table>
| PEM (Base64-encoded ASCII text) | PKCS #7 protocol P7B file | A certificate chain containing the following:  
  - A signed certificate for the system, authenticating its public key  
  - The CA's public certificate  
  - Intermediate certificates (optional)  
  To install the certificate, upload the file or paste the certificate text into the text box. |
| CER (single certificate) file | A signed certificate for the system, authenticating its public key  
To install the certificate, upload the file or paste the certificate text into the text box. |
Certificate procedures include the following:

- Install your chosen CA's public certificate so that the RealPresence Access Director system trusts that CA.
- Create a certificate signing request for a public certificate that identifies the RealPresence Access Director system and submit the request to the CA.
- When you receive the public certificate signed by your CA, install it on your RealPresence Access Director system.
- When necessary, remove a signed certificate or a CA's certificate.

**Note: Deploying two systems in a tunnel configuration**
If you have deployed two systems in a tunnel configuration, the tunnel connection between the tunnel server and client uses a default self-signed certificate dedicated for tunnel use. The key length is 2048 bits. This certificate cannot be changed but can be refreshed from the web user interface before it expires.

**View Installed Certificates**
The Certificates main page lists all certificates in the RealPresence Access Director system.

**To view installed certificates:**

- Go to Admin > Certificates.

  The following table describes the certificate information that displays.
You can view detailed information about each certificate in the RealPresence Access Director system.

To view detailed information about certificates:

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

**Certificate Details** displays the following information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate Info</strong></td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td>The purpose of the certificate for the RealPresence Access Director system.</td>
</tr>
<tr>
<td></td>
<td>• 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. You must create a certificate signing request 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. <strong>Note:</strong> Only one Server SSL certificate can exist in the system at one time; adding a new Server SSL certificate will replace the old one.</td>
</tr>
<tr>
<td></td>
<td>• CA is the root certificate of the certificate authority that the RealPresence Access Director system trusts. The system will treat the self-signed certificates from trusted peers as CA certificates.</td>
</tr>
<tr>
<td>Key usage</td>
<td>Indicates the operations that can be performed using the public key contained in the certificate.</td>
</tr>
<tr>
<td>Extended key usage</td>
<td>Indicates the purpose of the public key contained in the certificate. It contains a list of object identifiers (OIDs), each of which indicates an allowed use.</td>
</tr>
<tr>
<td><strong>Issued To</strong></td>
<td></td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>For a Server SSL certificate, the fully qualified domain name (FQDN) of the system’s management interface, as defined in the <strong>Hostname</strong> and <strong>Domain</strong> fields in <strong>Admin &gt; Network Settings &gt; General Network Setting</strong>. For a CA certificate, the common name of that certificate.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Usually, the legal name of your enterprise.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>The subdivision of your organization, such as Human Resources or IT, that creates and manages the certificate.</td>
</tr>
<tr>
<td>Serial number</td>
<td>The certificate serial number.</td>
</tr>
<tr>
<td><strong>Subject Alternative Name</strong></td>
<td>Lists the IP address and DNS name of each Subject Alternative Name (SAN) included on the single certificate. <strong>Note:</strong> If you configure access proxy settings for HTTPS proxies and specify next hops using the Host header filter, you must add the host FQDNs as Subject Alternative Names when you create a certificate signing request for the RealPresence Access Director system.</td>
</tr>
<tr>
<td><strong>Issued By</strong></td>
<td></td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>The common name of the entity that issued the certificate.</td>
</tr>
</tbody>
</table>
The Online Certificate Status Protocol (OCSP) is a protocol used to obtain the revocation status of an X.509 digital certificate. When this feature is enabled, the RealPresence Access Director system checks a certificate’s AuthorityInfoAccess (AIA) extension fields for the location of an OCSP responder. If no OCSP responder is found, the certificate fails validation. Otherwise, the RealPresence Access Director system sends the OCSP request to the responder identified in the certificate.

To use the Online Certificate Status Protocol (OCSP):

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

   The **Confirm Action** dialog displays two possibilities:
   - Access proxy restarts if you click **Yes** to save the configuration. This does not require a restart of the entire system.
   - The system restarts if you click **Yes** to save the configuration while SIP service is enabled.

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

Add a Certificate Authority’s Public Certificate

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

To add the certificate of a trusted root CA:

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

   The installed certificates are listed. The CA entries, if any, represent the certificate authorities whose public certificates are already installed on the RealPresence Access Director system and are trusted.

2. If you’re using a certificate authority that isn’t listed, access the certificate authority of your choice and obtain a copy of the CA’s public certificate.

   The certificate must be either a single certificate or certificate chain. If it’s ASCII text, it’s in PEM format, and starts with the text `-----BEGIN CERTIFICATE-----`. If it’s a file, it can be either PEM or DER encoded.
3. Go to Admin > Certificates > Add Certificates.

4. In the Add Certificates dialog, 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, 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.

**Note: Importing self-signed TLS/SSL peer certificates**

Self-signed TLS/SSL peer certificates are treated as CA certificates when you import them into the RealPresence Access Director system.

## Create a Certificate Signing Request

After initial installation, the RealPresence Access Director system is configured to use a self-signed certificate with a key length of 2048 bits. You can create a certificate signing request (CSR) to apply for a signed certificate from a certificate authority to replace the self-signed certificate. The signed certificate identifies the RealPresence Access Director system as a trusted entity.

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

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

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

**Note: Adding host FQDNs as Subject Alternative Names**

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

### To create a certificate signing request:

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

   If a signing request has already been created, the system asks if you want to use the existing request or generate a new one. Click Generate New to generate a new request.
2 In the **Certificate Information** dialog, enter the identifying information for your RealPresence Access Director system, as described in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Common Name (CN)</td>
<td>Defaults to the fully qualified domain name (FQDN) of the RealPresence Access Director system’s management interface, as specified in Admin &gt; Network Settings.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain name of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>SAN List (0&lt;=size&lt;=20)</td>
<td>Optional Subject Alternative Names, which can be IPv4 addresses or FQDNs. Specifying SANs in the CSR allows additional IP addresses and/or FQDNs to be protected with just one certificate.</td>
</tr>
<tr>
<td></td>
<td>If you create HTTPS reverse proxy next hops using the Host header filter (e.g., for the Polycom® RealPresence® CloudAXIS™ Suite Services Portal or Experiences Portal), you must specify the host FQDNs as Up to 20 SANs can be specified in the certificate signing request.</td>
</tr>
<tr>
<td></td>
<td>SANs. See Configure HTTPS Proxy Settings.</td>
</tr>
<tr>
<td></td>
<td>• To add a SAN, click the + (plus) icon and enter the IPv4 address or FQDN.</td>
</tr>
<tr>
<td></td>
<td>• To delete a SAN, select it and click the X (delete) icon.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Each time you add or revise a SAN, you must submit a new CSR.</td>
</tr>
<tr>
<td>Organizational unit (OU)</td>
<td>The subdivision of your organization, such as Human Resources or IT, that creates and manages the certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can enter up to 128 characters in this field but not all characters may display after you</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Typically, the legal name of your enterprise.</td>
</tr>
<tr>
<td>City or locality (L)</td>
<td>The city where your enterprise is located.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>The state where your enterprise is located.</td>
</tr>
<tr>
<td>* Country (C)</td>
<td>Two-character ISO code for the country in which your enterprise is located.</td>
</tr>
</tbody>
</table>

3 **Click OK.**

4 From the Certificate Signing Request dialog, 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-----
```
Submit the CSR.

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

Click OK to close the dialog.

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

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

Review the Signed 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.

Caution: Attempting to install an invalid certificate

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

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

To review the certificate:

1. Check the following certificate details:

<table>
<thead>
<tr>
<th>Certificate Field</th>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid from/Valid to</td>
<td>Check the validity period of the certificate to ensure that it is not expired and is currently valid.</td>
</tr>
<tr>
<td></td>
<td>Note: Ensure the certificate is valid for the selected time zone.</td>
</tr>
</tbody>
</table>
Add the Signed Certificate to the KEY_STORE

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

Caution: Changing certificates requires a system restart
When you install your CA-signed certificate, the certificate KEY_STORE is updated immediately; however, the RealPresence Access Director system does not apply the update until you restart the system. When you restart the system, all active calls are terminated and users are logged out of 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 following table describes the potential error messages.

<table>
<thead>
<tr>
<th>Cause of Error</th>
<th>Error Message</th>
</tr>
</thead>
</table>
| 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. |
To add the signed certificate to the KEY_STORE:

1. Go to Admin > Certificates > Add Certificates.
2. In the Add Certificates dialog, 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, 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.

Refresh the Server SSL Self-Signed Certificate

The Server SSL self-signed certificate can be renewed before it expires.

Caution: Refresh replaces a signed or self-signed certificate
If you have installed a signed certificate to identify your RealPresence Access Director system, clicking Refresh will replace the CA-signed certificate with a new self-signed certificate. In this case, you must apply for and install a new signed certificate to replace the Server SSL self-signed certificate.

To renew the KEY_STORE Server SSL self-signed certificate:

1. Go to Admin > Certificates.
2. Select the Server SSL self-signed certificate and click Refresh.
   
   The certificate is renewed for one year.

Add a Certificate from a Trusted Connection

You can install the CA certificates of trusted servers, other devices, or federated connections.

To add a certificate from a trusted connection:

1. Go to Admin > Certificates > Add Certificates.
2. In the Add Certificates dialog, 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, click OK to restart the system.

The certificate is added to the TRUSTED_STORE.

Replace a Signed Certificate

You can replace signed certificates when necessary.

To replace a signed certificate:

1 Complete the signing request procedure described in Create a Certificate Signing Request.

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.

6 Click OK.

7 In the Confirm Action dialog, click OK to restart the system.

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

Delete a Certificate

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

Note: Some certificates cannot be deleted

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.

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.

3 Click Delete Certificate.

4 In the Information dialog, click OK.

5 In the Confirm Action dialog, click Yes to restart the system.
Provision the System

When the RealPresence Access Director system is integrated with a Polycom RealPresence Resource Manager system, the RealPresence Resource Manager system can provision remote endpoints if the endpoints are registered with the RealPresence Resource Manager system. Additionally, some of the settings for the RealPresence Access Director system can be provisioned. See Connect to the RealPresence Resource Manager System for instructions.

For specific details on provisioning, see Polycom Unified Communications in RealPresence Access Director System Environments and the Polycom RealPresence Resource Manager System Operations Guide for your version of the RealPresence Resource Manager system.

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

Connect to the RealPresence Resource Manager System

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

Note: Provisioning not supported in the RealPresence Access Director, Virtual Edition

The RealPresence Access Director system, Virtual Edition cannot be provisioned by a RealPresence Resource Manager system. You must manually configure all access proxy settings. Note that the RealPresence Access Director system, Virtual Edition does enable endpoint provisioning by a RealPresence Resource Manager system.

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.

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

3. Click Connect.

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

Polycom, Inc. 73
To disconnect from the RealPresence Resource Manager System:

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

Integrate with Microsoft Active Directory

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

- Enables you to map roles to Active Directory groups rather than to individual users. See Use Role Mapping Settings.
- Allows Active Directory users who have been assigned a role to log into the RealPresence Access Director system by entering their Active Directory credentials.

**Note: Supports one domain, no subdomains**
The RealPresence Access Director system supports one Active Directory domain and does not support subdomains.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory server address</td>
<td>The IP address or FQDN of the Active Directory server.</td>
</tr>
<tr>
<td>Domain\User name</td>
<td>The domain and user name that the RealPresence Access Director system uses to log into Active Directory and retrieve domain and group information.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that the RealPresence Access Director system uses to log into Active Directory.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Optional. Base distinguished name (DN) is the top level of the LDAP directory. Specify the base DN in the following form (case insensitive):&lt;br&gt;DC=Polycom, DC=com&lt;br&gt;The RealPresence Access Director system fetches Active Directory domains from the specified base DN.</td>
</tr>
</tbody>
</table>
Use Role Mapping Settings

Role mapping enables you to assign a user role (administrator, auditor, or provisioner) to members of an 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.

To add a group and assign a mapping role:

1. Go to Admin > Microsoft Active Directory.
2. Ensure that Enable integration with Microsoft Active Directory Server is selected.
3. Click Add and provide the following information:
   - Group name in Active Directory—Enter the name of the Active Directory group. A name can include letters, numbers and the dash (-), underscore (_), and backward slash (\) special characters
   - Mapping Role: Select the role to assign to the Active Directory group.
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**.

**Configure SIP Signaling Settings**

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

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

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

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Port Number</th>
<th>Transport Type</th>
<th>Certificate</th>
<th>Dial String Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unencrypted</td>
<td>5060</td>
<td>UDP/TCP</td>
<td>Not required</td>
<td></td>
</tr>
<tr>
<td>Encrypted</td>
<td>5061</td>
<td>TLS</td>
<td>Not required</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

The system also has default internal SIP port settings used for communication to and from the RealPresence DMA system, which acts as the SIP server. The following table lists the internal port settings.

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Default Port Number</th>
<th>Transport Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unencrypted</td>
<td>5070</td>
<td>UDP/TCP</td>
</tr>
<tr>
<td></td>
<td>5070</td>
<td>TCP</td>
</tr>
<tr>
<td>TLS port (encrypted)</td>
<td>5071</td>
<td>TLS</td>
</tr>
</tbody>
</table>

**Configure SIP Settings**

You can configure specific SIP settings to support video conferencing calls to and from your enterprise network.
To configure SIP settings:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Port Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Port number</td>
<td>The external listening port the RealPresence Access Director system uses</td>
<td><em>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.</em>*</td>
</tr>
<tr>
<td>* Port name</td>
<td>The descriptive name for the port.</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol of the port.</td>
<td></td>
</tr>
<tr>
<td>Require certificate from remote endpoint</td>
<td>This option is available only for TLS transport. When enabled, the</td>
<td><strong>Note</strong>: This option must be enabled if the port will be used for a SIP federation.</td>
</tr>
<tr>
<td>Default contact port for SIP open B2B</td>
<td>The listening port the RealPresence Access Director system uses to receive SIP requests from endpoints that are not registered or are not members of a federated enterprise or division. The RealPresence Access Director system routes SIP open B2B calls only if you specify a valid default contact port for each type of transport. The default SIP ports are: TCP, UDP: 5060 TLS over TCP: 5061 You can designate other unused ports as the default contact ports if preferred. Only one default contact port can be configured for each type of transport.</td>
<td></td>
</tr>
<tr>
<td>Dial string policy</td>
<td>When enabled, the RealPresence Access Director system uses a dial string prefix to route incoming SIP messages from the external port to a RealPresence DMA system.</td>
<td></td>
</tr>
<tr>
<td>Prefix of Userinfo</td>
<td>The dial string prefix that the RealPresence Access Director system adds to the request line of the SIP INVITE message that is routed to the RealPresence DMA system. <strong>Note</strong>: This dial string prefix must also be defined in the RealPresence DMA system.</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>Specifies the host IP address or FQDN to use in the dial string. <strong>Caution</strong>: If you define a new host, or edit an existing host, you must also define the host in the RealPresence DMA system. If its host is not defined, the DMA system will reject calls from the new host.</td>
<td></td>
</tr>
</tbody>
</table>
### Internal Port Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Unencrypted port</td>
<td>The transport protocol the RealPresence Access Director system uses for unencrypted SIP calls and the internal listening port the system uses for SIP signaling messages from the RealPresence DMA system. Default UDP/TCP port: 5070. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>* TLS port</td>
<td>The internal listening port the RealPresence Access Director system uses for TLS-encrypted SIP signaling messages from the RealPresence DMA system. Default TLS port: 5071. <strong>Note:</strong> Polycom recommends that you use the default port number, but you can use any value from 5060–5100 or 65400–65499 that is not already in use and is different from the UDP/TCP port. If SIP signaling is enabled, TLS is automatically supported.</td>
</tr>
</tbody>
</table>

### Other SIP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* SIP registrar (Next hop) address, Port, and Transport</td>
<td>The IP address or FQDN of the SIP registrar server, and the destination port number and transport protocol the system uses to communicate with the SIP registrar server. The port number of the SIP registrar server must be the same as the port on which the SIP server in the RealPresence DMA system listens. The transport protocol must be supported by the SIP registrar server. Default TCP and UDP port: 5060. Default TLS port: 5061. Default transport protocol: TCP. <strong>Note:</strong> Polycom recommends that you use the default port number 5060 for UDP and TCP, and port number 5061 for TLS; however, you can use any value from 5060–5100 or 65400–65499 that is not already in use. When AUTO is selected, the transport protocol depends on the DNS query result for the SIP registrar address. Only the TCP and TLS transport options are available if you select TCP in the <strong>Unencrypted port</strong> field.</td>
</tr>
</tbody>
</table>
Add an External SIP Port Setting

You can configure external SIP port settings with different parameters for SIP connections.

To add an external port:

1. Go to Configuration > SIP Settings.
2. Select Enable SIP signaling.

---

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* SIP proxy (Next hop) address, Port, and Transport</td>
<td>The IP address or FQDN of the internal SIP proxy server to which the RealPresence Access Director system routes SIP registration requests or SIP call requests from endpoints. The RealPresence DMA system acts as the SIP proxy server so this is the DMA system IP address. The port number of the SIP proxy server must be the same as the port on which the SIP server in the RealPresence DMA system listens. The transport protocol must be supported by the SIP proxy server. <strong>Note</strong>: Polycom recommends that you use the default port number (5060) for UDP and TCP, and port number 5061 for TLS; however, you can use any value from 65400–65499 that is not already in use. When AUTO is selected for transport, the transport protocol depends on the DNS query result for the SIP proxy address. Only the TCP and TLS transport options are available if you select TCP in the Unencrypted port field.</td>
</tr>
<tr>
<td>* Registration refresh interval</td>
<td>Specifies how often registered SIP endpoints send keep-alive messages to the SIP registrar server to refresh the existing registration. Endpoints that fail to send keep-alive messages on time must send a new registration request. This value must be greater than or equal to the minimum SIP registration interval that the SIP registrar server allows. <strong>Default</strong>: 300 seconds <strong>Range</strong>: 1–99999 seconds</td>
</tr>
<tr>
<td>* RFC5626 keep-alive interval</td>
<td>The number of seconds (Flow-Timer value) after which the SIP registrar considers a call dead if no keep-alive message is sent by an RFC5626 endpoint. <strong>Default</strong>: 120 seconds <strong>Range</strong>: 1–99999 seconds</td>
</tr>
<tr>
<td>Skip validating TLS certificate from remote server</td>
<td>When enabled, the RealPresence Access Director system accepts TLS certificates from remote servers or other devices and allows outgoing TLS calls to proceed. However, the RealPresence Access Director system does not validate the certificates of the remote devices.</td>
</tr>
</tbody>
</table>

4. Click Update to save the settings. The SIP service restarts.
3 Click Add next to the External Port Settings list.
4 Complete the external port settings as described in the table in Configure SIP Settings.
5 Click OK.
6 Click Update.

Edit an External SIP Port Setting
External SIP port settings can be edited as needed.

To edit an external SIP port:
1 Go to Configuration > SIP Settings.
2 Select the port to edit in the External Port Settings table.
3 Click Edit.
4 Modify the port information as needed.
5 Click OK.
6 Click Update.

Delete an External SIP Port
Delete external SIP port settings that are no longer in use.

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

Configure H.323 Signaling Settings
The RealPresence Access Director system supports the H.323 protocol for call signaling and control for videoconferencing sessions.
When a remote H.323 client sends a registration request to the RealPresence Access Director system, the system proxies the registration request to the enterprise gatekeeper (the RealPresence DMA system) to enable the H.323 call.
The RealPresence Access Director system also supports remote H.323 users with H.460-enabled endpoints. The H.460.18 (signaling) and H.460.19 (media) standards enable traversal of H.323 signaling across firewalls and network address translators (NATs). To support H.460, the RealPresence Access Director system does the following:
● Uses the H.460.18 registration procedure to proxy registration requests from H.460-enabled endpoints to the gatekeeper.
● Enables the keep-alive mechanism of H.460.19 for opening and maintaining Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) pinholes in the firewall for communication between the remote endpoint and the gatekeeper.

**Note:** H.460 endpoints must use the same port to send and receive one media stream

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

**To configure H.323 settings:**

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

   An asterisk (*) indicates a required field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable H.323 signaling</td>
<td>Enables the system to operate as an H.323 server, transmitting H.323 requests and responses for H.323 endpoints. <strong>Caution:</strong> Disabling H.323 terminates any existing H.323 calls.</td>
</tr>
</tbody>
</table>

**Internal port settings**

| * H.225 RAS port         | The internal listening port the RealPresence Access Director system uses for receiving Registration, Admission, and Status (RAS) messages from the RealPresence DMA system gatekeeper. Default: 1719  
|                           | **Note:** Polycom recommends that you use the default port number, but you can use any value from 1700–1800 or 65400–65499 that is not already in use. |
| * H.225 call signaling port | The internal listening port the RealPresence Access Director system uses for receiving Q.931 signaling messages from the RealPresence DMA system gatekeeper. Default: 1720  
|                           | **Note:** Polycom recommends that you use the default port number, but you can use any value from 1700–1800 or 65400–65499 that is not already in use. |

**External port settings**

| * H.225 RAS port | The external listening port the RealPresence Access Director system uses for receiving Location Request (LRQ) messages to be forwarded to the RealPresence DMA system gatekeeper. Default: 1719  
|                 | **Note:** Polycom recommends that you use the default port number, but you can use any value from 1700–1800 or 65400–65499 that is not already in use. |
**Field** | **Description**
--- | ---
* H.225 call signaling port | The external listening port the system uses for receiving Q.931 signaling messages to be forwarded to the RealPresence DMA system gatekeeper. Default: 1720  
**Note:** Polycom recommends that you use the default port number, but you can use any value from 1700–1800 or 65400–65499 that is not already in use.

**General settings**

| Field | Description |
--- | ---|
* Gatekeeper (Next hop) address | The IP address or FQDN of the H.323 gatekeeper. |
* RAS port | The listening port of the RealPresence DMA system gatekeeper. The RealPresence Access Director system forwards LRQ messages to this port.  
**Note:** Polycom recommends that you use the default port range 0–65535. |
* H.225 call signaling port | The listening port of the RealPresence DMA system gatekeeper. The RealPresence Access Director system forwards Q.931 signaling messages to this port.  
**Note:** Polycom recommends that you use the default port range 0–65535. |

**CIDR**

| Field | Description |
--- | ---|
CIDR | In the RealPresence Access Director system, Classless Inter-Domain Routing (CIDR) notations include the IP address and subnet of local network H.323 devices (e.g., the RealPresence DMA system gatekeeper, endpoints, and bridges). You should add CIDR notations that specify all of the IP spaces within your enterprise LAN that include H.323 devices. |

**Bypass H.323 Federation Restrictions**

| Field | Description |
--- | ---|
Allow any incoming LRQ | When enabled, the RealPresence Access Director system forwards any incoming gatekeeper neighboring Location ReQuest (LRQ) to your enterprise’s gatekeeper (DMA system) without validating whether the source IP address belongs to a neighbored division or enterprise. |
Allow any outgoing LRQ | When enabled, the RealPresence Access Director system forwards any outgoing gatekeeper neighboring Location ReQuest (LRQ) from your enterprise’s gatekeeper (DMA system) without validating whether the destination address belongs to a neighbored division or enterprise. |
Enable H.323 guest policy | When enabled, the RealPresence Access Director system adds a prefix to the dial string when forwarding H.323 guest calls from an external network to the RealPresence DMA system.  
Default: disabled  
**Note:** If both Enable H.323 guest policy and Enable H.323 default policy are enabled, the RealPresence Access Director system uses the default destination alias you specify to forward H.323 guest calls to the RealPresence DMA system. |
Prefix to dial string | If H.323 guest policy is enabled, the RealPresence Access Director system adds the prefix you specify to the dial string when forwarding H.323 guest calls from an external network to the RealPresence DMA system. |
To add a CIDR address:

1. Go to Configuration > H.323 Settings.
2. In the CIDR fields, enter the IP address and the routing prefix size of the local network subnet that includes H.323 devices.
3. Click Add.
   The CIDR address displays in the CIDR list.
4. Enter a separate CIDR address for each subnet that has H.323 devices.

To delete a CIDR address:

1. Go to Configuration > H.323 Settings.
2. In the CIDR address list, select the IP address to delete and click Delete.

To enable H.323 default policy:

Select to enable the RealPresence Access Director system to assign a default destination alias to incoming H.323 guest calls that do not already include a destination alias in the Q.931 call SETUP message. The RealPresence Access Director system uses the default destination alias you specify to route H.323 guest calls to the RealPresence DMA system. The system uses two types of default aliases to associate a call from an H.323 guest endpoint with a specific gatekeeper:

- E.164
- H.323_ID

### H.460 settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable H.323 default policy</td>
<td>Select to enable the RealPresence Access Director system to assign a default destination alias to incoming H.323 guest calls that do not already include a destination alias in the Q.931 call SETUP message. The RealPresence Access Director system uses the default destination alias you specify to route H.323 guest calls to the RealPresence DMA system. The system uses two types of default aliases to associate a call from an H.323 guest endpoint with a specific gatekeeper: E.164, H.323_ID.</td>
</tr>
<tr>
<td>E.164</td>
<td>A default destination alias string that consists of numbers, e.g., a meeting room number or extension number.</td>
</tr>
<tr>
<td>H.323_ID</td>
<td>A default destination alias string that consists of alphanumeric characters, e.g., a meeting room name or customer’s name.</td>
</tr>
<tr>
<td>External registration refresh interval</td>
<td>Specifies how often registered endpoints send keep-alive messages to the RealPresence Access Director system to refresh the existing call registration. Endpoints that fail to send keep-alive messages on time must send a new registration request. Default value: 60 seconds Range: 15–150 seconds</td>
</tr>
<tr>
<td>Internal registration refresh interval</td>
<td>Specifies how often the RealPresence Access Director system sends keep-alive messages to the RealPresence DMA system to refresh the existing call registration. Default: 300 seconds Range: 150–9999 seconds</td>
</tr>
</tbody>
</table>

3. Click Update to save the settings.
TURN Services

Web Real-Time Communication (WebRTC) is a web-based communication technology that provides high-quality video and audio communication capabilities in some web browsers, without requiring installation of a custom plug-in. By using Google Chrome, users both inside and outside your enterprise network can attend web-based Polycom® RealPresence® Web Suite Pro conferences, in which media is exchanged directly between WebRTC clients (mesh conference) or between WebRTC clients and a Polycom RealPresence Collaboration Server Multipoint Control Unit (MCU).

To support WebRTC-based video conferencing, the RealPresence Access Director system implements both Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols. When needed, the RealPresence Access Director system can act as a STUN and TURN server to enable firewall and NAT traversal of UDP media traffic between WebRTC clients.

WebRTC clients use Interactive Connectivity Establishment (ICE) to establish traffic flows in environments where NAT and firewall traversal may be an issue. Using ICE, the clients determine the most efficient path to send media to each other. The possible paths include use of "host candidates" (where media can be sent to the client's local IP address), "server reflexive candidates" (where media can be sent to the client's public IP address hosted by an intervening firewall/NAT element) or a "relay candidate" (where media is sent to a TURN server, which relays the media to the local client).

A WebRTC client behind a firewall/NAT (and thus with a private IP address) uses STUN to discover its own public IP address and port on the firewall's external interface so it can communicate that address to a peer as a possible way for the peer to send media to the WebRTC client.

TURN is necessary when a WebRTC client wants to communicate with a peer but cannot do so due to both, client and peer, being behind respective NATs. STUN is not an option if one of the NATs is a symmetric NAT (a type of NAT known to be non-STUN compatible). TURN is also needed when direct UDP media cannot be exchanged for other reasons (for example, due to an organization's firewall policies). Using the TURN protocol, a WebRTC client can allocate a media relay port on the TURN server that the far end can use to indirectly send media to the WebRTC client.

When you enable and configure the TURN server and a TURN user, internal and external WebRTC clients can request TURN media relay services.

How Allocations Work

All TURN operations revolve around allocations, and all TURN messages are associated with an allocation. When a WebRTC client wants to communicate with a peer in a RealPresence Web Suite Pro WebRTC conference, the client sends an Allocate request to the TURN server. Once the TURN server authenticates the request, it creates an allocation and sends the client an Allocation Successful response, which contains, among other things, a relayed transport address that specifies the IP address and port on the TURN server that the WebRTC client and peer can use to have the TURN server relay media between them. An allocation is uniquely identified by its relayed transport address.

When the RealPresence Access Director system is deployed behind a NAT, the relayed transport address sent in the allocation response should always be the public IP address mapped on your firewall that corresponds to the IP address of the network interface you assigned to TURN services. This is true for responses sent to either the internal client or external client that sent the initial allocation request.

Typically, one allocation is created between the WebRTC client that initiates the allocation request and each peer with which it communicates. In a call with fewer than four endpoints (a WebRTC mesh call), an
allocation is required for each peer-to-peer connection. For example, if three users attend a conference, each peer typically has two allocations, one for each other peer on the call.

When an MCU hosts a WebRTC call, the TURN server relays media for the allocation between each WebRTC client and the bridge.

Once the TURN server creates allocations, you can view details about them by going to Diagnostics > TURN Allocations (see View TURN Allocations). Note that the number of allocations on the TURN server may not correspond with the number of calls in progress. Typically, each WebRTC client will create one TURN allocation for each peer with which it needs to connect. The ICE candidate selection process then determines the most efficient path available, so individual allocations may not be needed if the media can be sent directly to a host or server-reflexive address or through an existing TURN relay allocated by a peer client. Unused allocations will expire 10 minutes after media relay transfer begins. Typically, one allocation will remain active per leg for the duration of the call.

The RealPresence Access Director system supports up to 1200 allocations.

### Configure TURN Settings

When you configure TURN settings, Polycom recommends that you assign TURN services to the network interface assigned to external signaling. The external IP address (private) of this interface must be mapped to the public IP address on your firewall.

The number of dynamic ports you specify for TURN media relay doesn’t necessarily map to the number of calls that can be supported. The number of ports required to support all WebRTC calls varies depending on whether the conference uses mesh mode or bridge mode. The allowable port range is designed to accommodate a large number of licensed calls.

Polycom recommends that you use the default port range listed in the TURN Settings since the number of allocations can vary for calls, but you can choose any port range within the allowable range. The port range you configure must be configured on your firewall.

#### Create at least one TURN user

When you enable the TURN server for the first time, you must add at least one TURN user in order for the TURN server to allow requests. If you disable the TURN server, all TURN users are saved and will be available if you later re-enable the TURN server.

#### To configure TURN Server settings:

1. Go to Configuration > TURN Settings.
2. Select Enable TURN server.

   The TURN server is disabled by default for new installations of the RealPresence Access Director system.

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

<table>
<thead>
<tr>
<th>Settings</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listening IPs–Available IPs</td>
<td>The list includes the IP addresses of all network interfaces configured on your system.</td>
</tr>
</tbody>
</table>
**Settings** | **Field**
---|---
* Listening IPs—Selected IPs | The list displays the IP address of the network interface you assign to provide TURN services. You should select the network interface assigned to external signaling and map the external IP address (private) to the public IP address on your firewall, specified in **External IP Address of NAT**.
- Select the IP address from the Available IPs list, then click the right arrow to move the IP address to the **Selected IPs** list.
Assign TURN services to only one network interface.

* TURN port (UDP) | The listening port the RealPresence Access Director system uses to receive TURN allocation requests from internal or external clients.
Default UDP port: 3478
Allowable port range: 65370-65379

* Relay port range (UDP) | The port range used to relay media directly between WebRTC clients in a mesh call or between WebRTC clients and an MCU in a bridge call.
Default port range: 49152–65535
Allowable relay port range: 32768–65535
Polycom recommends that you use the default port range, but you can choose any port range within the allowable range that is not already in use. Each allocation requires one port, so if your port range is small, only a small number of allocations can be supported at one time.

* Default authentication realm | The realm is typically a domain name and is part of the required authentication credentials for a TURN user. If a WebRTC client provides only a username and password when requesting TURN services, the TURN server automatically assigns the default authentication realm.

External IP address of NAT | The public IP address for TURN, mapped on the external firewall. This field is required if you selected Deployed behind Outside Firewall with NAT when you configured your network settings. See Configure Network Interfaces.

**TURN Users**

| **Username** | A list of the usernames of each TURN user you create. |
| **Realm** | A list of the realms for each TURN user you create. |

4 Add at least one TURN user. See Add a TURN User.
5 Click **Update**.

![Warning icon] Click **Update** to save any TURN settings or TURN user information
Always click **Update** to save any changes you make to TURN Settings or TURN Users.

**TURN Users**
The TURN server requires authentication of all relay allocation requests. When the TURN server receives an unauthorized initial allocation request from a WebRTC or MCU client, the TURN server responds with its realm, which identifies the TURN user credentials a WebRTC client or MCU (TURN user) must use to
authenticate further requests with the TURN server. The credentials include the username and password to be used with the realm of the TURN server.

Configure identical TURN users on locally redundant systems
If you deploy two RealPresence Access Director systems for local redundancy, you must configure identical TURN users on each system if you enable the TURN servers.

Add a TURN User

You need to configure one TURN user to enable WebRTC clients to request TURN services for RealPresence Web Suite Pro mesh or bridge conferences. Once you configure the TURN user, you must share the credentials with the system administrator for the RealPresence Web Suite Pro system, who will complete further configurations for that product.

To add a TURN user:

1. Go to Configuration > TURN Settings.
2. Next to the list of TURN Users, click Add.
3. Complete the following required fields:
   - **Username**: the username that a WebRTC client uses to authenticate requests to the TURN server. Maximum of 20 characters.
   - **Realm**: the realm value is typically a domain name and is specific to the TURN server. When you configure one user for RealPresence Web Suite Pro WebRTC and MCU clients, the realm value should be the same as the Default Authentication Realm you configured in TURN Settings. The realm value uniquely identifies the username and password combination that a WebRTC client must use to authenticate its TURN requests. Maximum of 20 characters.
   - **Password**: the password that a WebRTC client uses in combination with the username to authenticate its TURN requests. Maximum of 20 characters.
   - **Verify Password**
4. Click OK to add the TURN user.
5. Click Update to save the TURN Users settings.

Configure Media Traversal Settings

The media relay component of the RealPresence Access Director system enables audio, video, and content traffic to traverse the firewall during SIP and H.323 calls.

To configure the media traversal settings:

1. Go to Configuration > Media Traversal Settings.
2. Configure the settings as described in the following table.
Configure 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, a server, or other device. For H.323 systems, this trust relationship is between mutually neighbored gatekeepers.

Note: Obtain and install the certificate of the other system before configuring a federation

Before you configure a SIP federation, you must obtain the CA certificate of the trusted server or device with which you will create the federation and install it in your RealPresence Access Director system’s TRUSTED_STORE. See Add a Certificate from a Trusted Connection.

For additional information about federations, see Federation Between RealPresence Access Director Systems and Federation Between RealPresence Access Director and Other Systems in Polycom Unified Communications in RealPresence Access Director System Environments.

3 Under Actions, click Update to save the settings.

For more information on configuring media traversal settings, refer to Polycom Unified Communications in RealPresence Access Director System Environments.
To view current enterprise federations:

1. Go to Configuration > Federation Settings.

The system displays details about currently federated companies or divisions, as shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the company name with which you have a federated connection</td>
</tr>
<tr>
<td>Company Address</td>
<td>The domain name or IP address of the federated company</td>
</tr>
<tr>
<td>First Remote Listen Port</td>
<td>SIP: The remote listening port of the trusted SIP peer H.323: The H.225 RAS port of the trusted H.323 neighbor</td>
</tr>
<tr>
<td>Second Remote Listen Port</td>
<td>SIP: Not applicable H.323: Remote H.225 signaling port</td>
</tr>
<tr>
<td>Local Contact Port</td>
<td>The port on the local RealPresence Access Director system used for incoming SIP calls from the federated company. <strong>Note:</strong> Local ports used for incoming calls from a SIP federation must be configured for mutual TLS communication. This means that the RealPresence Access Director system will accept the certificate of the federated company during incoming calls. See External Port Settings in Configure SIP Settings.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of federated connection (SIP or H.323)</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the connection (Active or Inactive)</td>
</tr>
</tbody>
</table>

Search for a Federation

Use the search function to find a specific federation.

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.

Add a Federation

To establish a trusted connection with an external enterprise or division, you can create a federation with the other enterprise.

**Note:** Configure access control lists to allow incoming calls from federations

After you add a federation, you must configure the appropriate call policy settings in Basic Access Control Lists to allow incoming calls from federations. See Configure Call Policy Settings.

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>The name of the company in the federated relationship.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of federated connection (SIP or H.323).</td>
</tr>
<tr>
<td>Company Address</td>
<td>The domain name or IP address of the federated company.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The numeric prefix that the RealPresence Access Director system assigns to the SIP server and gatekeeper of the federated enterprise. When prefixes are assigned, callers from your enterprise can dial the prefix of the SIP server or federated enterprise gatekeeper plus the alias of the destination. You can reuse the same prefix for a single SIP federated connection and an H.323 neighbor; however, the prefix for each SIP federated connection and each H.323 neighbor must be unique. Example: Prefix 77 can be assigned to both SIP federation 1 and H.323 neighbor 1. Prefix 77 cannot be assigned to SIP federation 2 or H.323 neighbor 2.</td>
</tr>
<tr>
<td>Strip Prefix</td>
<td>When selected, the RealPresence Access Director system removes the prefix from the dial string.</td>
</tr>
<tr>
<td>Remote Listen Port</td>
<td>SIP only The listening port of the trusted SIP peer.</td>
</tr>
<tr>
<td>Remote H.225 RAS Port</td>
<td>H.323 only The H.225 RAS port of the trusted neighbored gatekeeper or H.323 proxy. Applicable for H.323 only.</td>
</tr>
<tr>
<td>Remote H.225 Signaling Port</td>
<td>H.323 only The H.225 call signaling port of the trusted neighbored gatekeeper or H.323 proxy.</td>
</tr>
<tr>
<td>Local Contact Port</td>
<td>The listening port on the local RealPresence Access Director system for the SIP trunk or H.323 gatekeeper connection. <strong>Note</strong>: The local port used for incoming calls from a SIP federated peer must be configured for mutual TLS communication. This means that the RealPresence Access Director system will validate the certificate of the federated company during incoming calls. See <strong>External Port Settings</strong> in Configure SIP Settings.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the connection (<strong>Active</strong> or <strong>Inactive</strong>).</td>
</tr>
<tr>
<td>Strip Host Domain</td>
<td>H.323 only When selected, the RealPresence Access Director system removes the domain name from a dial string, then interprets the dial string as an E.164 number or H.323 ID and forwards the call to the next hop.</td>
</tr>
</tbody>
</table>

4 Click **OK**.
Edit a Federation Setting

You can revise federation settings if information about the other enterprise or division changes.

To edit a federation setting:

1. Go to Configuration > Federation Settings.
2. Under Actions, click Edit.
3. In the Edit Company window, revise the federation settings as needed.
4. Click OK to save the new settings.
System Administration and Additional Settings

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

- High Availability Settings
- Set Custom Security for Network Access
- Configure Port Range Settings
- Configure Log Settings
- SNMP Overview
- Configure SNMP Settings
- Configure History Retention Settings
- Define Advanced Access Control List Rules
- Use Variables in Access Control List Rules
- Apply Rule Settings to Access Control List Rules

High Availability Settings

Two RealPresence Access Director systems can be configured on the same network to provide High Availability (HA) of services. Systems configured for High Availability support minimal interruption of services and greater call reliability.

In an HA configuration, each RealPresence Access Director system has a virtual IP address for at least one network interface with assigned services. Each virtual IP address maps to the public IP address for external signaling configured on the firewall. If one RealPresence Access Director system fails, the peer system takes over the failed system’s resources (virtual IP addresses and assigned services). All active calls are either dropped automatically or callers must manually hang up, but registration and provisioning information for endpoints is maintained in memory and shared between both systems. Once all resources are re-established on the peer system, users can call back into the video conference without changing any call information.

Although not required, Polycom recommends that you configure more than one network interface as an HA link. Multiple HA links ensure fewer points of failure and provide a reliable mechanism for communication between the two systems.
Configure High Availability Settings

When you configure High Availability settings on one system, you can synchronize the settings to the other system by using the Configure Peer option.

To configure High Availability settings:

1. Go to Admin > High Availability Settings.
2. Select Enable High Availability (HA).
3. Use the information in the following table to configure the settings for your system.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Local Physical IP Address</td>
<td>IP address of the selected local network interface. Each network interface you configured in network settings displays as a tab (eth0, eth1, etc.). Select the appropriate tab to configure specific HA settings, if any, for each network interface.</td>
</tr>
<tr>
<td>Local Virtual IP Address</td>
<td>The virtual IP address of the selected local network interface. The <strong>Local Physical IP Address</strong>, <strong>Local Virtual IP Address</strong>, and <strong>Peer Virtual IP Address</strong> must be on the same subnet for the selected interface. Note that if the selected network interface has assigned services, the virtual IP address will inherit the same service bindings. <strong>Note</strong>: This field is required only on network interfaces with signaling and access proxy traffic assigned that are not enabled as HA links.</td>
</tr>
</tbody>
</table>
After you configure each network interface, click Submit. The system reboots.
After the system restarts, go to Admin > High Availability Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Virtual Hostname</td>
<td>Virtual hostname of the selected interface. Example: ha-rpad-1-0 A hostname can contain the following characters: a–z A–Z 0–9 - . (periods are allowed only in domain style names) Blank spaces and underscores are not allowed. Note: This field is required only on network interfaces with signaling and access proxy traffic assigned that are not enabled as HA links.</td>
</tr>
<tr>
<td>Peer Virtual IP Address</td>
<td>Virtual IP address of the same network interface on the peer system. Note: This field is required only on network interfaces with signaling and access proxy traffic assigned that are not enabled as HA links.</td>
</tr>
<tr>
<td>Peer Virtual Hostname</td>
<td>Virtual hostname of the same network interface on the peer RealPresence Access Director system. Example: ha-rpad-2-0 Note: This field is required only on network interfaces with signaling and access proxy traffic assigned that are not enabled as HA links.</td>
</tr>
</tbody>
</table>

**HA Communication Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Interface for HA Traffic | When enabled:  
  • The network interface serves as an HA link and communicates with the peer system via the peer’s physical IP address for the same network interface.  
  • You must enter the Peer Physical IP Address.  
  • If only media is assigned to a network interface, you cannot enable it as an HA link.  
  At least one network interface must be enabled as an HA link. Polycom recommends enabling two network interfaces as HA links if you do not use at least one direct link. |
| Use Direct Link             | Select this option if you have a direct, physical link (crossover or Ethernet cable) between the same network interface on both systems. Use Direct Link cannot be enabled on network interfaces that have assigned services. |
| Peer Physical IP Address    | The physical IP address of the same network interface on the peer RealPresence Access Director system. Note: This field is required on network interfaces that you enable as HA links. |

**Configured Services**

| Each network interface      | Displays the services assigned to each network interface you select. |

---

4. After you configure each network interface, click Submit. The system reboots.
5. After the system restarts, go to Admin > High Availability Settings.
6 Click **Configure Peer** to apply the same settings to the peer system.
7 Complete the following fields. Note that all fields are required:
   - **Peer IP**: Enter the management IP address of the peer RealPresence Access Director system.
   - **Peer Port**: Port 8443 is the default port for the peer system.
   - **Peer Admin Account**: The username that the peer system administrator uses to log in to the system’s web user interface.
   - **Peer Admin Password**: The peer system administrator’s login password.
   - Click **OK**.

**Change HA Password**

When you configure two RealPresence Access Director systems for High Availability, the two systems share an internal account that supports authentication between the systems. The account does not require any interaction. However, if your network policy requires you to change passwords at certain intervals, you can use the **Change HA Password** option.

- **Do not change the HA password if either system has active calls**
  Change the HA password only when both systems have no active calls. Otherwise, all active calls will be dropped when you submit the changes from the High Availability Settings page.

**To change the HA password:**

1 Go to **Admin > High Availability Settings**.
2 Click **Change HA Password**.
3 Enter the new password and confirm the password.
4 Click **OK**.
5 Click **Submit**.
   The peer system reboots.
6 After the peer system restarts, go to **Admin > High Availability Settings**.
7 Click **Configure Peer**.
8 Enter the name and password and click **OK**.
   The peer system reconnects and all HA settings are applied to the peer system, including the new password.

**View High Availability Status Details**

See **View High Availability Status**.

**Set Custom Security for Network Access**

Custom security settings enable you to specify options for controlling network access. Note that only administrators can enable and disable custom security settings.

- **Allow Linux SSH access**—When enabled, allows remote Secure Shell access to the RealPresence Access Director system console.
● **Enable access proxy white list authentication for LDAP and XMPP access**—When enabled, the RealPresence Access Director system denies all LDAP and XMPP requests from endpoints that are not provisioned by a RealPresence Resource Manager system.

● **Enforce TLS for LDAP connection**—When enabled, the RealPresence Access Director system denies all LDAP connection requests sent from remote endpoints without TLS encryption.

  **Caution: Enable the Enforce TLS for LDAP connection option**
  This option is enabled by default. Polycom strongly recommends that you disable this setting *only* if you need backward compatibility with Polycom RealPresence Group Series 300/500 endpoints that have not been upgraded to the most recent software version. Endpoints that have not been upgraded do not use an encrypted TLS connection when requesting LDAP services.

To enable or disable network access methods:
1. Go to Admin > Security Settings.
2. Select or clear the custom security options.
3. Click Update.
4. Click Yes to confirm your selections.

**Configure Port Range Settings**

This section describes the dynamic port ranges to configure for the RealPresence Access Director system and correspondingly on your firewall.

The RealPresence Access Director system automatically calculates dynamic port ranges based on the number of calls for which you are licensed. A port range for a specific function indicates the number of ports for that function that must be available to accommodate the number of calls on your system license. You can change the beginning port ranges (within certain parameters) if necessary. If you change a beginning port range number for signaling, Binary Floor Control Protocol (BFCP)/TCP content, or media, the RealPresence Access Director system automatically calculates the end port number for that service based on your number of licensed calls.

Dynamic port ranges configured for the RealPresence Access Director system must be configured correspondingly on your firewall.

  **Caution: Ports configured in the RealPresence Access Director system must match your firewall ports**
  The specific ports and port ranges you configure in the RealPresence Access Director system must match the ports configured on your firewall. If you change any port settings within the system, you must also change them on your firewall.

You can configure ranges for the following ports:

- H.323 dynamic ports
- SIP dynamic source ports
- External BFCP/TCP ports
- Internal BFCP/TCP ports
Access proxy dynamic source ports (This feature is not related to the number of calls on a license and the full range of ports is available by default. You can specify both the beginning and end port numbers to limit the range for access proxy.

External media ports

Internal media ports

Note: BFCP/TCP ports support content streaming through HTTP tunnel proxy
The RealPresence Access Director system allocates TCP ports for BFCP traffic. The BFCP/TCP ports are used exclusively to support content streaming through the HTTP tunnel proxy for RealPresence Web Suite users.

The following table summarizes general port information, the number of ports the RealPresence Access Director system reserves for each type of port, and an example port range on a system licensed for 100 calls.

<table>
<thead>
<tr>
<th>Service</th>
<th>Transport</th>
<th>Number of Ports Reserved</th>
<th>Beginning Port Number</th>
<th>Ending Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 dynamic ports</td>
<td>TCP</td>
<td>Number of licensed calls X 3</td>
<td>10001</td>
<td>10300</td>
</tr>
<tr>
<td>SIP dynamic source ports</td>
<td>TCP</td>
<td>Number of licensed calls X 2</td>
<td>13001</td>
<td>13200</td>
</tr>
<tr>
<td>External BFCP/TCP ports</td>
<td>TCP</td>
<td>Number of licensed calls</td>
<td>15001</td>
<td>15100</td>
</tr>
<tr>
<td>Internal BFCP/TCP ports</td>
<td>TCP</td>
<td>Number of licensed calls</td>
<td>16001</td>
<td>16100</td>
</tr>
<tr>
<td>Access proxy dynamic source ports</td>
<td>TCP</td>
<td>Variable Each dynamic mode client uses three ports (HTTPS provisioning, LDAP, and XMPP presence). Each RealPresence Web Suite client, and Polycom ContentConnect client use one port.</td>
<td>30001</td>
<td>60000</td>
</tr>
<tr>
<td>External media ports</td>
<td>UDP</td>
<td>Number of licensed calls X 10</td>
<td>20002</td>
<td>21001</td>
</tr>
<tr>
<td>Internal media ports</td>
<td>UDP</td>
<td>Number of licensed calls X 10</td>
<td>40002</td>
<td>41001</td>
</tr>
</tbody>
</table>

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

- No end port number is greater than 60000.
- No beginning port number is less than 10000.
- No overlap occurs between the port ranges for TCP transport and no overlap occurs between the port ranges for UDP transport if the ports are configured for the same IP address.
To configure the port range settings:

1. Go to Admin > Port Range Settings.
   If you have not activated your license for an Appliance Edition system, the default settings for a five-call trial license display.
2. Enter the beginning port number for the port range you want to change.
   The system automatically updates the ending port number value.
3. Click Update and confirm the changes.
   The system confirms that the update was successful.

Configure 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.

Note: System logging part of Polycom’s Management Instrumentation Solution
Support for system logging is part of Polycom’s management instrumentation solution. For detailed information on using the manageability instrumentation solution with your Polycom products, see the Polycom RealPresence Manageability Instrumentation Solution Guide.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log file rolling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rolling frequency</td>
<td>The frequency at which the system rolls active log files into archive files.</td>
<td>Every day</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Retention period (days)</td>
<td>The number of days that the system retains archived log files before deleting them.</td>
<td>7 days</td>
</tr>
<tr>
<td></td>
<td>Range: 1-30 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Polycom recommends downloading archived log files before the end of the retention period.</td>
<td></td>
</tr>
<tr>
<td>Application log settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging level</td>
<td>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.</td>
<td>Info</td>
</tr>
<tr>
<td>Log file size</td>
<td>The size of the log file.</td>
<td>50 MB</td>
</tr>
<tr>
<td></td>
<td>Range: 1-50 MB</td>
<td></td>
</tr>
</tbody>
</table>
Configure Log File Rolling and Application Log Settings

Configure these settings to specify the rolling frequency, retention period, and logging level for the log files.

Log settings do not apply to TURN server logs

The settings you configure for log file rolling, applications logs, and remote syslog do not apply to any TURN server logs.

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

1. Go to Admin > Log Settings.
2. Complete 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 value.
   - The **logging level** that you select generates messages as described in the following table:

<table>
<thead>
<tr>
<th>Logging Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug</td>
<td>Detailed information used to debug the system. Using this level captures more information but consumes a higher level of system resources. If you set the logging level to Debug to capture details for debugging, set the logging level back to the default Info when you finish debugging.</td>
</tr>
<tr>
<td>Info</td>
<td>Normal operational messages that highlight the progress of the system and do not require any action. Info is the default logging level.</td>
</tr>
<tr>
<td>Warn</td>
<td>Warning messages that indicate an error will occur if action is not taken.</td>
</tr>
</tbody>
</table>
Log file size—Maximum size you specify for each log file, ranging from 1 to 50 MB.

Configure Remote Syslog Settings

Remote syslog settings identify the location and other details about the remote server where log files are stored.

To add a remote syslog server:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>The transport protocol the system uses to send log files to the remote server. Default value is UDP.</td>
</tr>
<tr>
<td>Remote address</td>
<td>The IP address of the remote server where the log files will be stored.</td>
</tr>
<tr>
<td>Remote port</td>
<td>The listening port for syslog-ng on the remote system.</td>
</tr>
<tr>
<td>Severity filter</td>
<td>The event severity filter to apply to the remote syslog server.</td>
</tr>
<tr>
<td></td>
<td>Debug</td>
</tr>
<tr>
<td></td>
<td>Info (default)</td>
</tr>
<tr>
<td></td>
<td>Notice</td>
</tr>
<tr>
<td></td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>Err</td>
</tr>
<tr>
<td></td>
<td>Crit</td>
</tr>
<tr>
<td></td>
<td>Alert</td>
</tr>
<tr>
<td></td>
<td>Emerg</td>
</tr>
</tbody>
</table>

4. In Source log files, select the Available source files for syslog-ng to store as local log files and forward to the remote server:
   - ACCESSPROXY
   - ACTIVECALLAUDITOR
   - DBACCESS
   - H323SERVICE
   - LICENSE
   - SIPSERVICE
SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of resources in a network.

Note: SNMP support part of Polycom’s Management Instrumentation Solution
Support for SNMP and system logging is part of Polycom’s management instrumentation solution. For detailed information on using the manageability instrumentation solution with your Polycom products, see the Polycom RealPresence Manageability Instrumentation Solution Guide.

SNMP Framework

The SNMP framework has three parts:

- **An SNMP manager**
  
  The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. A variety of network management applications are available for use with SNMP. It is important to note that you should understand how your SNMP management system is configured to properly configure your Polycom system SNMP transport protocol requirements, SNMP version requirements, SNMP authentication requirements, and SNMP privacy requirements. For information on using SNMP management systems, see the appropriate documentation for your application.

- **An SNMP agent**
  
  The SNMP agent is the software component within the Polycom system that maintains the data for the system and reports these data, as needed, to managing systems. The agent and MIB reside on the same system.

- **A MIB**
  
  The MIB (Management Information Base) is a virtual information storage area for network management information, which consists of collections of managed network objects. You can configure the SNMP agent for a particular system MIB. The agent gathers data from the MIB, the repository for information about system parameters and network data. Polycom systems include Polycom-specific MIBs with every system as well as third-party MIBs. Polycom MIBs are self-documenting, including information about the purpose of specific traps and inform notifications. Third-party MIBs accessible through the Polycom system may include both hardware and software system MIBs.

SNMP Versions

Polycom supports two versions of SNMP:
● **SNMPv2c**—Polycom implements a sub-version of SNMPv2. SNMPv2c uses a community-based form of security. The community of SNMP managers able to access the agent MIB is defined by an IP-based Access Control List and password.

One drawback of SNMPv2c is that it is subject to packet sniffing of the clear text community string from the network traffic, because it does not encrypt communications between the management system and SNMP agents.

● **SNMPv3**—Polycom implements the newest version of SNMP. Its primary feature is enhanced security. SNMPv3 provides secure access to systems with a combination of authenticating and encrypting packets over the network. The `contextEngineID` in SNMPv3 uniquely identifies each SNMP entity. The `contextEngineID` is used to generate the key for authenticated messages. Polycom implements SNMPv3 communication with authentication and privacy (the `authPriv` security level as defined in the USM MIB).

- Authentication is used to ensure that traps are read by only the intended recipient. As messages are created, they are given a special key that is based on the `contextEngineID` of the entity. The key is shared with the intended recipient and used to receive the message.
- Privacy encrypts the SNMP message to ensure that it cannot be read by unauthorized users.
- Message integrity ensures that a packet has not been tampered with in transit.

**SNMP Notifications**

A key feature of SNMP is the ability to generate notifications from an SNMP agent. Notifications are called as such because they are sent, unsolicited and asynchronous to the SNMP manager from the Polycom system. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to another system, or other significant events. They are generated as informs or trap requests.

Traps are messages alerting the SNMP manager to a system or network condition change. Inform requests (informs) are traps that include a request for a confirmation receipt from the SNMP manager. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. However, informs consume more system and network resources. Traps are discarded as soon as they are sent. An inform request is held in memory until a response is received or the request times out. Traps are sent only once while informs may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and network resources.
Configure SNMP Settings

Configure the general SNMP settings, then add notification users and notification agents as needed.

To configure SNMP settings:

1. Go to Admin > SNMP Settings.
2. Select Enable SNMP monitoring.
3. Configure the following settings for the connection between the RealPresence Access Director system and the SNMP agent.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SNMP Version** | Specifies the version of SNMP you want to use. Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocol:  
  v2c—Used for standard models. Uses community-based authentication.  
  v3—Used when you want a high security model. Requires a security user for notifications.  
  Because UDP doesn't have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring. |
| **Transport** | Specifies the transport protocol for SNMP communications. SNMP can be implemented over two transport protocols:  
  TCP—This protocol has error-recovery services, message delivery is assured, and messages are delivered in the order they were sent. Some SNMP managers only support SNMP over TCP.  
  UDP—This protocol does not provide error-recovery services, message delivery is not assured, and messages are not necessarily delivered in the order they were sent.  
  Because UDP doesn't have error recovery services, it requires fewer network resources. It is well suited for repetitive, low-priority functions like alarm monitoring. |
| **Port**     | Specifies the port that the RealPresence Access Director system uses for general SNMP messages. By default, the RealPresence Access Director system uses port 161. |
| **Community** | For SNMPv2c, specifies the context for the information, which is the SNMP group to which the devices and management stations running SNMP belong. The RealPresence Access Director system has only one valid context—by default, public—which is identified by this Community name. The RealPresence Access Director system will not respond to requests from management systems that do not belong to its community. |
Configure Notification Users

For SNMPv3 notifications, you must specify at least one security user. Security users are authorized to receive notifications (Traps or Informs).

Add a Notification User

After enabling SNMP monitoring in the RealPresence Access Director system, if you select v3 as the SNMP version, you must add the first security user on the Agent Setting tab. See the settings described in To add an SNMP notification user.

You can add additional notification users from the Notification Setting tab.

To add an SNMP notification user:

1. Go to Admin > SNMP Settings > Notification Setting.
2. Click Add User.
3. Configure the following settings in the Add Notification User dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security user</td>
<td>The user name of the security user authorized to actively retrieve SNMP data.</td>
</tr>
</tbody>
</table>
| Authentication type     | The authentication protocol used to create unique fixed-sized message digests of a variable length message. The RealPresence Access Director system implements communication with authentication and privacy (the authPriv security level, as defined in the USM MIB). Authentication type options:  
  • MD5–Creates a digest of 128 bits (16 bytes)  
  • SHA–Creates a digest of 160 bits (20 bytes)  
  Both methods include the authentication key with the SNMPv3 packet and then generate a digest of the entire SNMPv3 packet. |
| Authentication password | The authentication password that’s used, together with the local engine ID, to create the authentication key included in the MD5 or SHA message digest. |
| Confirm password        |                                                                                               |
Edit a Notification User

You can revise notification user details as needed.

To edit a notification user:

1. Go to Admin > SNMP Settings > Notification Setting.
2. Select the user and click Edit User.
3. Modify the settings in the Add Notification User dialog as needed.
4. Click OK to save the settings.

Delete a Notification User

Delete notification users when you no longer want them to receive SNMP notifications.

To delete a notification user:

1. Go to Admin > SNMP Settings > Notification Setting.
2. Click Delete User.
3. Click Yes to confirm the deletion.

Configure Notification Agents

You can configure notification agents by specifying the notification receivers and the types of notifications an agent sends. To limit the effect on system performance, you can add a maximum of eight agents.

Add a Notification Agent

Use the Add Notification Agent dialog to add an SNMP agent to the RealPresence Access Director system.

To add an SNMP notification agent:

Go to Admin > SNMP Settings > Notification Setting.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption type</td>
<td>The privacy protocol for the connection between the RealPresence Access Director system and the SNMP agent.</td>
</tr>
<tr>
<td></td>
<td>Encryption type options:</td>
</tr>
<tr>
<td></td>
<td>• No encryption</td>
</tr>
<tr>
<td></td>
<td>• DES—Uses a 56-bit key with a 56-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td></td>
<td>• AES—Uses a 128-bit key with a 128-bit salt to encrypt the SNMPv3 packet</td>
</tr>
<tr>
<td>Encryption password</td>
<td>The password that’s used, together with the local engine ID, to create the encryption key used by the privacy protocol.</td>
</tr>
<tr>
<td>Confirm password</td>
<td></td>
</tr>
</tbody>
</table>
1 Click Add Agent.
2 Configure the settings in the Add Notification Agent dialog box.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable agent</td>
<td>Select to enable the notification agent. Clear to stop using this agent without deleting it.</td>
</tr>
<tr>
<td>Transport</td>
<td>The transport protocol for SNMP communications to the host receiver (TCP or UDP).</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the host receiver (the SNMP manager to which this agent sends notifications).</td>
</tr>
<tr>
<td>Port</td>
<td>The port that the RealPresence Access Director system uses to send notifications. Default port–162</td>
</tr>
</tbody>
</table>
| Notification type | The type of notification that this agent sends to the notification receiver:  
  • Inform–The agent sends an unsolicited message to a notification receiver and expects or requires the receiver to respond with a confirmation message.  
  • Trap–The agent sends an unsolicited message to a notification receiver and does not expect or require a confirmation message. |
| SNMP version   | The version of SNMP used for this agent (v2c or v3). |
| Security user  | For SNMP v3, the user name of the security user authorized to actively retrieve SNMP data. |

3 Click OK.
   The agent appears in the Notification Agents list.

**Edit a Notification Agent**

Revise notification agents as needed when agent settings change.

**To edit a notification agent:**
1 Go to Admin > SNMP Settings > Notification Setting.
2 Select the agent to edit and click Edit Agent.
3 Modify the settings in the Edit Notification Agent dialog as needed.
4 Click OK to save the settings.

**Delete a Notification Agent**

Delete notification agents if they are no longer valid.

**To delete a notification agent:**
1 Go to Admin > SNMP Settings > Notification Setting.
2 Select the agent to delete and click Delete Agent.
3 Click Yes to confirm the deletion.
Download MIBs

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INET-ADDRESS-MIB</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>polycom-access-management</td>
<td>The RealPresence Access Director system-specific MIB definition.</td>
</tr>
<tr>
<td>POLYCOM-BASE-MIB</td>
<td>Base MIB for Polycom products.</td>
</tr>
<tr>
<td>SNMPv2-CONF</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-SMI</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
<tr>
<td>SNMPv2-TC</td>
<td>A definition file for standard conventions included for reference.</td>
</tr>
</tbody>
</table>

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

**To download a MIB:**

1. Go to **Admin > SNMP Settings**.
2. Under **Actions**, click **Download MIBs**.
3. Select the MIB and click **Download**.
4. In the **Save As** window, navigate to where you want to save the MIB file locally and click **Save**.
5. Click **Close** to close the File Download window, and then click **OK**.

Configure History Retention Settings

Configure the History Retention Settings to specify when the system purges call and registration history data. According to the values you specify for retention, the system purges the oldest registration history, call history, and registration signaling message records when the number of records exceeds the maximum number to retain or when the records have been stored for the maximum number of days.

**Note: Purging call history or records also purges all associated data**

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

Some types of call signaling messages are not recorded in call history, including SIP OPTION and SIP INFO.
The following table describes the fields on the **History Retention Settings** page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable recording of registration</td>
<td>Enables the system to retain registration history records.</td>
</tr>
<tr>
<td>history</td>
<td>Default: Enabled</td>
</tr>
<tr>
<td></td>
<td>Registration history records to retain</td>
</tr>
<tr>
<td></td>
<td>Default: 250,000</td>
</tr>
<tr>
<td></td>
<td>Range: 50,000–500,000</td>
</tr>
<tr>
<td>Registration signaling message</td>
<td>The number of system registration signaling message records the system</td>
</tr>
<tr>
<td>records to retain</td>
<td>retains before purging the oldest records.</td>
</tr>
<tr>
<td></td>
<td>Default: 1,000,000</td>
</tr>
<tr>
<td></td>
<td>Range: 10,000–1,000,000</td>
</tr>
<tr>
<td>Enable recording of registration</td>
<td>Enables the system to retain SIP registration refresh and H.323 lightweight</td>
</tr>
<tr>
<td>refresh</td>
<td>Default: Disabled</td>
</tr>
<tr>
<td></td>
<td>Call history records to retain</td>
</tr>
<tr>
<td></td>
<td>Default: 250,000</td>
</tr>
<tr>
<td></td>
<td>Range: 50,000–500,000</td>
</tr>
<tr>
<td>History record purge interval</td>
<td>How often the system checks the number of registration and call history</td>
</tr>
<tr>
<td></td>
<td>records to see if they exceed the maximums. When the maximum number of</td>
</tr>
<tr>
<td></td>
<td>records to retain is reached, the system purges the excess.</td>
</tr>
<tr>
<td></td>
<td>Default: Every 30 minutes</td>
</tr>
<tr>
<td></td>
<td>Range: 5–1,440 minutes</td>
</tr>
<tr>
<td>The retention of history records</td>
<td>The number of days that the system keeps system registration and call history</td>
</tr>
<tr>
<td>according to time</td>
<td>records before purging the records that are older than the maximum number</td>
</tr>
<tr>
<td></td>
<td>of days specified.</td>
</tr>
<tr>
<td></td>
<td>Default: Every 90 days</td>
</tr>
<tr>
<td></td>
<td>Range: 10–180 days</td>
</tr>
</tbody>
</table>

**To configure history record retention:**

1. Go to **Admin > History Retention Settings**.
2. Specify the number of each type of record to retain in the system.
3. Specify how often you want the system to purge records in excess of those numbers.
4. Click **Update**.
   A dialog informs you that the configuration has been updated.
5. Click **Set as Default** to keep the settings you entered as the default values.
Define Advanced Access Control List Rules

Access Control Lists serve as filters for inbound SIP and H.323 traffic from the Internet to the RealPresence Access Director system’s external signaling ports. The ACL rules and associated settings define whether the RealPresence Access Director system allows or denies SIP or H.323 registration and call requests from endpoints or other devices on a public network.

The Access Control List feature provides numerous options for defining access rules and is highly configurable. You can use Access Control List rules and settings to create whitelists, blacklists, and other access controls. Additionally, multiple Access Control List rules can be applied on one port.

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

1. Define an Access Control List rule and its conditions. See Add an Access Control List Rule and Conditions.
2. Specify variables to apply to the Access Control List rules (optional). See Add a Variable.
   Note that if you plan to use custom variables for a rule condition, you should define the variables first, before you create or edit the rule and its conditions.
3. Apply the Access Control List rule and the associated action (rule setting) to a specific external port. See Add an Access Control List Setting and Rule Setting.

The Access Control List Rules page displays the following Access Control List rules:

- Basic Access Control List rules that the RealPresence Access Director system automatically created based on the settings you configured in Configure Basic Access Control List Settings.
- RealPresence Access Director system default rules (see Use the Default Access Control List Rules).
- Custom Access Control List rules that you create.

Note that rules the RealPresence Access Director system automatically creates based on your Basic ACL Settings are labeled Basic. The default system rules and custom rules that you configure are labeled Advanced.

When you select a rule from the rules list, information displays about that rule, as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Rule Name      | Name of the rule  
Note: A rule name cannot contain blank spaces. |
| Service        | Type of service to which the rule applies  
SIP, H.323, or Common (both services) |
| General Info   |                                                   |
| Name           | When you select a Rule Name, the name of the rule displays under General Info. |
| Description    | Description of the rule you selected              |
The following topics describe the actions you can perform from the Access Control List Rules page.

- Use the Default Access Control List Rules
- Add an Access Control List Rule and Conditions
- Copy an Access Control List Rule
- Edit or Delete an Access Control List Rule
- Edit or Delete a Condition for an Access Control List Rule

**Use the Default Access Control List Rules**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Condition   | Lists conditions for the rule you selected. A condition includes an attribute, operator, and value. If a rule has more than one condition, a relation defines how the conditions are applied relative to each other:  
  - **and**–If a message meets all of the conditions in the rule, the action for the rule is applied to the message.  
  - **or**–If a message meets any one of the conditions in the rule, the action for the rule is applied to the message.  
  - **and** and **or** display as folders. Click the folder to display all attributes for the relation. |
| Attribute    | When you select a condition, the attribute, operator, and value for the condition display. Attributes specify the fields in a SIP or H.323 request message. |
| Operator     | An operator compares the Attribute and Value fields of the condition. For any attribute you choose, the operator you select determines the available values for the condition. |
| Value        | The values that can be selected for a condition are dependent on the attribute and operator. |
The following table lists the default Access Control List rules included in the RealPresence Access Director system. Select a rule from the list of rules on the **Access Control List Rules** page to view its configuration and conditions.

### Default Access Control List Rules

<table>
<thead>
<tr>
<th>Name of Rule</th>
<th>Description</th>
<th>Service</th>
</tr>
</thead>
</table>
| Access_Without_Resource Manager_Provision | The RealPresence Access Director system records all IP addresses of remote endpoints and adds them to a provisioning list if the endpoint is authenticated during the VC2 provisioning process. When this rule is applied on a port, all incoming requests from IP addresses that are not on the provisioning list are accepted or denied, depending on the rule setting you apply.  
**Example:** Use this rule to deny access for SIP and H.323 services to endpoints not on the provisioning list. For instance, apply this rule on SIP port 5060 and assign **deny** as the rule setting action.  
**Note:** If two endpoints are behind the same Firewall/NAT, both may share one public IP address. If one endpoint is provisioned and the other is not, this rule is not applied and both endpoints are able to access port 5060. | Common |
| All_Matches                          | When this rule is applied to a port, all incoming requests on that port are accepted or denied, depending on the rule setting you apply.  
**Example:** Use this rule to change the default access policy. For example, a port is accessible by default without any access policy. To change the default behavior so that access is denied, apply this rule to the port and assign **deny** as the rule setting action. | Common |
| H323_Guest_Call                      | When this rule is applied to an H.323 call signaling port, all incoming H.323 call requests on the port from non-registered H.323 guest endpoints are accepted or denied, depending on the rule setting you apply.  
**Example:** Use this rule to reject guest H.323 calls from the Internet to an H.323 signaling port. For example, apply this rule on H.323 port 1720 and assign **deny** as the rule setting action. | H.323   |
| H323_Guest_Call_Not_To_71xxxx_bridge | When this rule is applied to an H.323 call signaling port, all incoming H.323 guest call requests on that port that match the dial string in the rule are accepted or denied, depending on the rule setting you apply.  
**Example:** Use this rule to allow guest H.323 calls from the Internet to access *only* the 71xxxx bridge. For example, apply this rule on H.323 port 1720 and assign **deny** as the rule setting action. | H.323   |
### Default Access Control List Rules

<table>
<thead>
<tr>
<th>Name of Rule</th>
<th>Description</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H323_Register_Call</strong></td>
<td>When this rule is applied to an H.323 RAS port, all incoming H.323 call requests on the port from registered H.323 endpoints are accepted or denied, depending on the rule setting you apply. <strong>Example:</strong> Use this rule to allow incoming H.323 call requests from registered H.323 endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign <strong>accept</strong> as the rule setting action.</td>
<td>H.323</td>
</tr>
<tr>
<td><strong>H323_Registration</strong></td>
<td>When this rule is applied to an H.323 RAS port, all incoming H.323 registration requests on the port from H.323 endpoints are accepted or denied, depending on the rule setting you apply. <strong>Example:</strong> Use this rule to allow incoming H.323 registration requests from H.323 endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign <strong>accept</strong> as the rule setting action.</td>
<td>H.323</td>
</tr>
<tr>
<td><strong>H323_Registration_Without_Polycom_Endpoint</strong></td>
<td>When this rule is applied to an H.323 RAS port, all incoming H.323 registration requests on the port from non-Polycom H.323 endpoints are accepted or denied, depending on the rule setting you apply. This rule has conditions that distinguish a Polycom endpoint's product ID from other vendors in the RRQ. <strong>Example:</strong> Use this rule to allow incoming H.323 registration requests from non-Polycom endpoints. The conditions for the rule specify that the vendor IDs do not match Polycom RealPresence Desktop, RealPresence Group, RealPresence Mobile, and HDX endpoints. For instance, apply this rule on H.323 RAS port 1719 and assign <strong>accept</strong> as the rule setting action.</td>
<td>H.323</td>
</tr>
<tr>
<td><strong>SIP_FriendlyScanner</strong></td>
<td>When this rule is applied to a SIP port, all incoming SIP requests on that port that contain the user-agent header value <strong>friendly-scanner</strong> are accepted or denied, depending on the rule setting you apply. <strong>Example:</strong> Use this rule to deny incoming SIP requests that contain the user-agent header value <strong>friendly-scanner</strong>. For example, apply this rule on SIP port 5061 and assign <strong>deny</strong> as the rule setting action.</td>
<td>SIP</td>
</tr>
<tr>
<td><strong>SIP_Guest_Call</strong></td>
<td>When this rule is applied to a SIP call signaling port, all incoming SIP call requests on the port from non-registered SIP guest endpoints are accepted or denied, depending on the rule setting you apply. <strong>Example:</strong> Use this rule to reject SIP guest calls from the Internet to a SIP signaling port. For example, apply this rule on SIP port 5061 and assign <strong>deny</strong> as the rule setting action.</td>
<td>SIP</td>
</tr>
</tbody>
</table>
Add an Access Control List Rule and Conditions

You can add new Access Control List rules and specify the conditions (attribute, operator, value) that define each rule.

To add a new Access Control List rule and conditions:

2. Enter a name for the rule, such as SIP_Call_Blacklist.
   Do not use blank spaces in the name.
3. Select the type of service and enter a description of the rule.
   For the example rule name above, select SIP as the service type.
4. Click Add to add a condition for the rule and select the Attribute, Operator, and Value for the condition. The following table illustrates an example of a condition for the rule SIP_Call_SIP_Reg_List.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Example String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Select the type of request for which the rule applies</td>
<td>request.from</td>
</tr>
<tr>
<td>Operator</td>
<td>Select the operator that indicates what the value must be in relation to the attribute.</td>
<td>memberOf</td>
</tr>
<tr>
<td>Value</td>
<td>Select from the list of predefined values for specific attributes, or select a custom variable. See Add a Variable.</td>
<td>var_Blacklist (custom variable)</td>
</tr>
</tbody>
</table>

5. Click OK to add the condition to the rule.
6. Add other conditions to the rule as needed.
Click OK to return to the Access Control List Rules page.

Configure the Access Control List settings as described in Add an Access Control List Setting and Rule Setting.

Copy an Access Control List Rule

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

To copy an Access Control List rule:

1. Go to Configuration > Access Control List Rules and select the Access Control List rule to copy from the Rule Name list.
2. Under Actions, click Copy.
3. Enter a new name for the rule and revise, add, or delete the conditions as needed.
4. Click OK to create the new rule.

Edit or Delete an Access Control List Rule

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

To edit an Access Control List rule:

1. Go to Configuration > Access Control List Rules and select the Access Control List rule to edit from the Rule Name list.
2. Under Actions, click Edit.
3. Revise the General Info as needed.
4. Click OK to save the changes to the Access Control List rule.
   To edit conditions for an Access Control List rule, see Edit or Delete a Condition for an Access Control List Rule.

To delete an Access Control List rule:

1. Go to Configuration > Access Control List Rules and select the Access Control List rule to delete from the Rule Name list.
2. Under Actions, click Delete > Yes.
   The rule is deleted from the rule list.
Edit or Delete a Condition for an Access Control List Rule

Conditions for an Access Control List can be edited as needed or deleted.

To edit a condition for an Access Control List rule:

1. Go to Configuration > Access Control List Rules and select the Access Control List rule that has the condition you want to edit.
2. Under Actions, click Edit.
3. Select the condition to revise and click Edit.
4. Select new definitions for the condition as needed.
5. Click OK to save the revised condition information.
6. Select and edit other conditions if necessary.
7. Click OK to save the changes to the Access Control List rule.

To delete a condition for an Access Control List rule:

1. Go to Configuration > Access Control List Rules and select the Access Control List rule with the condition(s) to delete.
2. Under Actions, click Edit.
3. Select the condition to delete and click Delete.
   The condition is removed from the Access Control List rule.
4. Click OK to save the changes to the Access Control List rule.

Example: Define an Access Control List Rule to Deny SIP Calls from Specific IP Addresses

Use this rule and settings to block SIP calls from a black list of IP addresses.

To deny SIP call requests from specific IP addresses on an external port:

1. Go to Configuration > Access Control List Variables and click Add.
2. Complete the following fields:
   - Name–Enter a name for the variable, such as BlacklistIPs. Do not use spaces in the name.
   - Value–Enter a value to include in the variable—in this case, an IP address.
3. Click Add to add the value to the values list.
4. Add other values as needed.
5. Click OK.
   The new variable displays in the Access Control List Variables list.
7. Click Add to create a new rule.
8. Enter a name for the rule, such as SIP_Blacklist. Do not use blank spaces in the name.
9. Select SIP and enter a description of the rule.
10 Click Add and select the following options:
   ➢ Attribute—request.src-ip
   ➢ Operator—memberOf
   ➢ Value: the name of the variable you created, such as var_BlacklistIPs
11 Click OK to add the condition.
12 Click OK to create the rule.
13 Click Access Control List Settings under Navigation.
14 Click Add and select the following options:
   ➢ Service Name—SIP
   ➢ IP—The external signaling IP address
   ➢ Port—The external SIP port for which the system will deny SIP calls from the blacklist you defined, e.g., 5061.
15 Click Add and select the following options:
   ➢ Access Control List Name—the rule you created to forbid SIP registration, such as SIP_Blacklist
   ➢ Action—deny
16 Click OK.
   The setting displays in the Rule Setting list.
17 Click OK to apply the setting to the Access Control List rule.

Use Variables in Access Control List Rules

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

Note: Create variables before defining rules

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

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Associated Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>prov_list</td>
<td>All endpoints that are successfully provisioned by the RealPresence Resource Manager system through the RealPresence Access Director system.</td>
<td>src.ip</td>
</tr>
</tbody>
</table>
These variables cannot be edited and are automatically updated by the RealPresence Access Director system.

### Add a Variable

You can create variables to be used in conditions for Access Control List rules.

**To add an Access Control List variable:**

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

### Edit or Delete a Variable

Edit or delete variables when necessary.

**To edit an Access Control List variable:**

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

**To delete an Access Control List variable:**

1. Go to `Configuration > Access Control List Variables` and select the variable to delete.
2. Under **Actions**, click **Delete > Yes**.
   - The variable is deleted from the list of variables.

---

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Associated Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>h323_reg_list</td>
<td>All H.323 endpoints that successfully register through the RealPresence Access Director system.</td>
<td>src.address</td>
</tr>
<tr>
<td>sip_reg_list</td>
<td>All SIP endpoints that successfully register through the RealPresence Access Director system.</td>
<td>src.address</td>
</tr>
</tbody>
</table>
Apply Rule Settings to Access Control List Rules

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

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

See the following sections for configuration details and examples:

- Add an Access Control List Setting and Rule Setting
- Edit or Delete an Access Control List Setting
- Edit or Delete a Rule Setting

Add an Access Control List Setting and Rule Setting

From the Access Control List Settings page, you can view current Access Control List settings, create new settings, and edit or delete settings. All changes are effective immediately for new call requests. Active calls are not affected.

To add an Access Control List setting and rule setting:

1. Go to Configuration > Access Control List Settings and complete the following fields:
   - **Service Name**—Select SIP or H.323.
   - **IP**—Select the external signaling IP address.
   - **Port**—Select the external port to which the Access Control List rule applies.

2. Click **Add** and complete the following fields:
   - **Access Control List Name**—Select the Access Control List rule to use for this Access Control List setting.
   - **Action**—Select Accept or Deny.

3. Click **OK**.

   The setting displays in the Rule Setting list.

4. Repeat the previous steps to add additional rule settings.

5. Click **OK** to create the Access Control List setting.

To prioritize rule settings:

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

1. Go to Configuration > Access Control List Settings and select an Access Control List to prioritize its rule settings.

2. Under Actions, click Edit.

3. Select a rule setting and click Priority Up or Priority Down to increase or decrease the priority of the rule setting. Repeat until the rule settings are listed (prioritized) in the order you want.

4. Click OK to apply the order of priority for the rule settings.
Edit or Delete an Access Control List Setting

You can edit or delete an Access Control List setting when necessary.

Caution: Deleting Access Control List settings and rule settings
If you delete an Access Control List setting, its associated rule settings are also deleted.

To edit an Access Control List setting:

1. Go to Configuration > Access Control List Settings and select the Access Control List setting to edit.
2. Under Actions, click Edit.
3. Revise the following fields as needed:
   - Service Name: Select SIP or H.323.
   - IP: Select the external signaling IP address.
   - Port: Select the external port to which the Access Control List rule applies.
4. Click OK to save the new settings or edit the rule settings if needed, as described in Edit or Delete a Rule Setting.

To delete an Access Control List setting:

1. Go to Configuration > Access Control List Settings and select the Access Control List setting to delete.
2. Under Actions, click Delete > Yes.
   The setting is deleted from the list of Access Control List Settings.

Edit or Delete a Rule Setting

You can edit or delete a specific rule setting within an Access Control List setting.

To edit a rule setting:

1. Go to Configuration > Access Control List Settings and select the Access Control List setting that contains the rule setting you want to edit.
2. Under Actions, click Edit.
3. Select the Rule Setting to revise and click Edit.
4. Revise the following information as needed:
   - Access Control List Name: Select the Access Control List rule to use for this Access Control List setting.
   - Action: Select Accept or Deny.
5. Click OK to apply the revised rule setting.
6. Click OK again to update the Access Control List setting.
To delete a rule setting:

1. Go to Configuration > Access Control List Settings and select the Access Control List setting you want to delete.
2. Under Actions, click Edit.
3. Select the Rule Setting to delete and click Delete.
4. Click OK.
User Management

To enable administration and management of the system, the Polycom® RealPresence® Access Director™ system enables you to create and manage local user accounts and roles. See Manage Local User Accounts and User Roles for instructions.

Manage Local User Accounts and User Roles

The RealPresence Access Director system supports three user roles, each with its own set of privileges. When you create a local user account, you can assign one or more roles to the user. The following table provides a brief overview of each user role:

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

From the Users page, you can perform the following tasks:

- Change Your System Password on page 121
- Search for a Local User Account on page 122
- Add a Local User Account and Assign User Roles on page 122
- Edit and Delete Local User Account Information on page 123

Change Your System Password

To increase security, Polycom recommends changing your RealPresence Access Director system password on a regular basis.

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.

Search for a Local User Account

Both administrators and provisioners can search for local user accounts.

To search for a user account:

1 Go to User > Users.
2 To reveal search filters, click .
3 Enter search string parameters in any of the following fields as needed to refine your search:
   ➢ Search users
   ➢ User ID
   ➢ First name
   ➢ Last name
4 To search by a user’s role, click the down arrow in the Role field and select the role.
5 Click Search.
   ➢ For a string search, the system attempts to match the string you entered against the beginning of the value for which you are searching. For example, if you enter sa in the Search users field, the system displays users whose first name, last name, or user ID begins with sa.
   ➢ For a role search, the system displays all local user accounts that are assigned to the role that you selected.

Add a Local User Account and Assign User Roles

One administrator account is created when you install the RealPresence Access Director system. After you log in to the web user interface, Polycom strongly recommends that you create a new administrator user account with personal login information. After you add the new administrator account, you should then delete the original administrator account created during installation. You can add other user accounts as needed.

When you use the RealPresence Platform Director system to install an instance of the RealPresence Access Director, Virtual Edition, you must specify the administrator user credentials for the RealPresence Access Director system. The administrator credentials that you enter in the RealPresence Platform Director system MUST match the administrator credentials in the RealPresence Access Director system. Therefore, if you change the administrator user credentials in the RealPresence Access Director web user interface, you must update the credentials for that instance in the RealPresence Platform Director system. See the Polycom RealPresence Platform Director System Administrator Guide, available at support.polycom.com.

Only administrators can add user accounts.

To add a local user account and assign a user role:

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First name</td>
<td>User’s first name</td>
</tr>
<tr>
<td>Last name</td>
<td>User’s last name</td>
</tr>
<tr>
<td>User ID</td>
<td>User’s login name</td>
</tr>
<tr>
<td>Password</td>
<td>User’s system login password</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Repeat user’s system login password</td>
</tr>
</tbody>
</table>

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

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

6 Click **OK**.

7 If you add a new administrator account in the RealPresence Access Director, Virtual Edition, log out of the web user interface and enter the new administrator user credentials in the RealPresence Platform Director system.

   **Note:** System assigns Auditor as the default user role

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

---

**Edit and Delete Local User Account Information**

You can edit or delete user account when necessary. Note that one administrator account must always exist in the system; if the system has only one administrator account, it cannot be deleted.

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

Administrators can delete other user accounts, but cannot delete their own account.

   **Caution:** Deleting an account deletes all account data

Be aware of the following before deleting a user account:

- When you delete an account, all of the account data is removed from the system.
- When you delete the account of a user who is logged into the system, the user is not affected by the deletion. The deletion is completed when the user logs out, and the user will not be able to log into the system again.

**To edit user information:**

1 Go to **User > Users**.
2 Select a user account from the list.
3 Click **Edit**.
4 Revise the user information and role as needed.
5 Click **OK**.
To delete a user account:

1. Go to User > Users.
2. Select a user account from the list.
3. Click Delete.
4. In the Confirm Action dialog, click Yes to complete the action.
System Maintenance

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

- Upgrade the Software
- Shut Down and Restart the System
- Back Up and Restore the System

Upgrade the Software

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

Only administrators can upgrade or roll back system software versions.

The following topics describe the tasks you can complete from the Software Upgrade page:

- View Software Information
- Upload an Upgrade Package File
- Install an Uploaded Package File
- Upload and Upgrade at the Same Time
- Roll Back to the Previous Software Version

Caution: After an upgrade, delete Internet Explorer temporary files and cookies

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

View Software Information

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

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

The Software Upgrade page displays the following system information:

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

Upload an Upgrade Package File

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

If the upgrade requires a new license activation key code or codes, obtain and install them as described in Obtain a License Activation Key Code.

Note: New Activation key codes required for some upgrades
In general, you must request a new activation key when you update to a major release (for example, 3.x to 4.x) or minor release (for example, 4.0 to 4.2). You do not need an activation key when you update to maintenance release (for example, 4.1.1 to 4.1.2) or a patch release. Always read the product release notes for specific information about whether or not you'll need an activation key.

To upload a package file for later installation:
1. Go to Maintenance > Software Upgrade.
2. Under Actions, click Upload.
3. Select the upgrade package file, and click Open.
   The File Upload dialog indicates when the upload is complete.
4. Click Close.
   The Operation History displays the status of the upload. Additionally, Upgrade Package Details displays information about the upgrade file.

Install an Uploaded Package File

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

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

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

Caution: Creating a backup
Polycom recommends that you download backup files before beginning an upgrade.
Upgrades require a system restart, which terminates active calls and logs all users out of the system.

To install an uploaded upgrade package file:
1. Go to Maintenance > Software Upgrade.
2. Under Actions, click Upgrade.
3. Click Yes to confirm the system upgrade.
   The system notifies you that the upgrade is starting.
4. Click OK to log out.
   The user interface closes during the upgrade process.
5. After the upgrade is complete, open a new browser window and access the RealPresence Access Director system user interface.
   The End-user License Agreement displays.
6. Click Accept to advance to the login page.
7. Log into the system and go to Maintenance > Software Upgrade.
8. Review the System version and Operation History to confirm the upgrade was successful.

Upload and Upgrade at the Same Time
The RealPresence Access Director system can upload an upgrade file and automatically install it.

To upload and install an upgrade package file:
1. Go to Maintenance > Software Upgrade.
2. From the Actions menu, click Upload and Upgrade.
3. Navigate to the upgrade package file, and click Open.
   After the upload is complete, the upgrading procedure begins automatically and the user interface closes.
4. After the upgrade is complete, open a new browser window and access the RealPresence Access Director system user interface.
   The End-user License Agreement displays.
5. Click Accept to advance to the login page.
6. Log into the system and go to Maintenance > Software Upgrade.
7. Review the System version and Operation History to confirm the upgrade was successful.

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

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

Caution: Rolling back requires a system restart
Rolling back to a previous version requires a system restart, which terminates active calls and logs all users out of the system.

To roll back the system to the previous version:
1. Go to Maintenance > Software Upgrade.
2. Under Version Information, verify that the rollback version is correct.
3. From the Actions menu, click Roll Back.
4. In the **Confirm Action** dialog, click **Yes**.
The system notifies you that the roll back is starting.

5. Click **OK**.
The user interface closes during the rollback process.

6. After the rollback is complete, open a new browser window and delete temporary Internet files and cookies from Internet Explorer before accessing the RealPresence Access Director system user interface. See **Cannot Open RealPresence Access Director System User Interface**.

7. Log into the system and go to **Maintenance > Software Upgrade**, and review the following:
   - **System version**: The version that you rolled back to.
   - **Rollback version**: Since you just completed a rollback, no version should display.
   - **Operation History**: A list of the actions you’ve completed that confirms the rollback was successful.

---

**Shut Down and Restart the System**

Only administrators can shut down and restart the system.

Caution: Shutting down or restarting terminates active calls
Shutting down or restarting the system terminates 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, click **Yes**.
   All active calls are terminated and users are logged out.

**To restart the system:**

1. Go to **Maintenance > Shutdown and Restart**.
2. Click **Restart**.
3. In the **Confirm Action** dialog, click **Yes**.
   All active calls are terminated and users are logged out. Typically, service is restarted after about five minutes.

---

**Back Up and Restore the System**

Polycom strongly recommends that you regularly create backups of your RealPresence Access Director system and download these files to a local computer or server. Backup files contain configuration, application, and operating system data and can be used to restore your system to a previous configuration or, in some cases, to a previous version of the software.
From the RealPresence Access Director system’s Backup and Restore page, you can complete the following actions:

- Create a Backup File
- Download a Backup File
- Upload a Backup File
- Restore the System from a Backup File
- Remove a Backup File
- Migrate Data from a Backup File

To view general information about backup files:

» Go to Maintenance > Backup and Restore.

The following information displays for each backup file:

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

**Create a Backup File**

Create backup files regularly to store configuration, application, and operating system data. Log files are not included in backup files.

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.

**Download a Backup File**

Downloading backup files enables you to store the files on a local computer or server.
To download a backup file to a local system:

1. Go to Maintenance > Backup and Restore.
2. Select the backup file to download.
3. Under Actions, click Download Selected.
4. Select a location to store the file and click Save.
   The progress of the file download displays.
5. Click Close when the download is complete.

Upload a Backup File

You must upload a locally-stored backup file if you need to restore your system.

To upload a backup file to the system server:

1. Go to Maintenance > Backup and Restore.
2. Under Actions, click Upload.
3. Navigate to the locally saved backup file and click Open.
   The progress of the file upload displays.
4. Click Close when the upload is complete.

Restore the System from a Backup File

The restore function enables you to perform a full restoration of your system from a backup file. If necessary, you can restore a backup file from one RealPresence Access Director system to a different RealPresence Access Director system. The two systems will have the same configuration.

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

Note: Consider when to restore from a backup file
Restore from a backup only when the system has no active calls. Restoring terminates all calls and restarts the system.

To restore the system from a backup file:

1. Go to Maintenance > Backup and Restore.
2. If you haven’t already done so, upload the backup file to use to restore the system.
3. Select the file from the list of backup files.
4. Under Actions, click Restore Selected.
5. In the Confirm Action dialog, Click Yes to restore the system from the backup file you selected.

Remove a Backup File

As you create new backup files, you can remove older ones from your system.
To remove a backup file:

1. Go to **Maintenance > Backup and Restore**.
2. Select the backup file to remove from the RealPresence Access Director system.
3. Under **Actions**, click **Remove Selected**.
4. In the **Confirm Action** dialog, Click **Yes** to remove the backup file you selected.

**Migrate Data from a Backup File**

You can migrate application configuration and system configuration data from a backup file after you have installed a new version of the RealPresence Access Director system.

When you restore your system from a backup file, the backup file must be from the same version as the version you currently use. However, when you *migrate* configuration data from a backup file, the data is from the version of the system you were using prior to the version you recently installed.

When you migrate from a backup file, the following information is migrated to the new version of your system:

- Configuration data in the database
- Application configuration files, for example:
  - All configuration files under directory
  - System controller configuration files under directory
- OS configuration files
  - IP address
  - Default gateway
  - Host name
  - DNS configuration
  - Configuration of iptables
  - Network configuration
  - NTP configuration
  - Time zone configuration
  - Syslog configuration
  - Interface configuration under directory `/etc/sysconfig/network-scripts/
  - Routing configuration script

The following data is not migrated:

- Call history data in the database
- Registration data in the database
- Log files

To migrate a backup file:

1. Go to **Maintenance > Backup and Restore**.
2. Under **Actions**, click **Migrate**.
3 When prompted to continue, click **OK**.

4 Navigate to the backup file to migrate and click **Open**.
   
The system completes the data migration from the backup file and restarts.
System Diagnostics

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

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

- View Active Call Details
- Call History
- Audit Registration History
- View TURN Allocations
- Manage System Log Files
- Run Traffic Capture
- Ping a Device
- Run Traceroute
- View High Availability Status
- Use Polycom Utilities

View Active Call Details

Use the Active Calls function to view information about an active call or to troubleshoot call issues.

To view details about active calls:

1. Go to Diagnostics > Active Calls.
   - 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.
Call History

The call history function lets you view detailed records of calls and call signaling events.
The historical data that is available depends on the settings you configure for history retention. See Configure History Retention Settings.

Search for Call Records

The search pane above the call list lets you find calls that match the criteria you specify. The search feature supports a wildcard (*) search for the Originator and Dial string parameters.
The Start After and Start Before settings are always active and define the time range during which the calls you are searching for began. When setting the date/time range for your search, keep in mind that retrieving a large number of records can take some time.

To search for calls:

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

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

3. Click Search.

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

View Call Details

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

To view call details:

1. Go to Diagnostics > Call History and complete a search for call history records.
To view call event details:
1. Go to Diagnostics > Call History and complete a search for call history records.
2. From the search results, select a call and click Show Call Details under the Actions list.
3. Select Call Events to display all signaling events for the selected call.

To view subscription event details:
1. Go to Diagnostics > Call History and complete a search for call history records.
2. From the search results, select a call and click Show Call Details under the Actions list.

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

**Audit Registration History**

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

**Search for Registration Records**

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

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

**To search for device registrations:**

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start after</td>
<td>The time after which the call began.</td>
</tr>
<tr>
<td>Start before</td>
<td>The time before which the call began.</td>
</tr>
<tr>
<td>Signaling type</td>
<td>SIP or H.323</td>
</tr>
<tr>
<td>Alias</td>
<td>The originating device’s alias.</td>
</tr>
<tr>
<td>IP address</td>
<td>The originating device’s IP address.</td>
</tr>
</tbody>
</table>

3. Click **Search**.

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

**View Registration Details**

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

**To view registration information:**

1. Go to **Diagnostics > Registration History** and complete a search for device registrations records.
2. From the search results, select a registration record and click **Show Registration Details** under the **Actions** list. **Registration Info** displays the following detailed information about the selected registration record.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling</td>
<td>SIP or H.323</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the registered device.</td>
</tr>
<tr>
<td>Alias</td>
<td>The device’s alias.</td>
</tr>
<tr>
<td>Address</td>
<td>The device’s IP address and port number.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time and date that the device registered.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time and date that the device’s registration ended (blank if the device is still registered).</td>
</tr>
</tbody>
</table>

To view registration event details:

1. Go to **Diagnostics > Registration History** and complete a search for device registrations records.
2. From the search results, select a registration record and click **Show Registration Details** under the **Actions** list.
3. Select **Registration Events** to display the event information about the selected registration record.

<table>
<thead>
<tr>
<th>Event</th>
<th>Event Details</th>
<th>Description</th>
</tr>
</thead>
</table>
| Registration begin| Alias         | **SIP**
|                   |               | Specifies the SIP URI in the header of the SIP REGISTER message. |
|                   |               | **H.323**
|                   |               | Lists all aliases of a client terminal included in the RRQ message. |
| Signaling type    | SIP or H323   | **Direction**
|                   |               | Specifies if the registration was inbound or outbound. |
| Direction         |               |             |
### View TURN Allocations

The TURN Allocations page lists details about each active TURN allocation.

#### To view the active TURN allocations:

1. Go to **Diagnostics > TURN Allocations**.
2. The following information displays for each allocation:

<table>
<thead>
<tr>
<th>Event</th>
<th>Event Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signaling</td>
<td>Event type</td>
<td>Indicates if the event was a request or a response, and the direction of the response (inbound or outbound).</td>
</tr>
<tr>
<td></td>
<td>Far end</td>
<td>The IP address and port of the far end from which the system received a signaling message.</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td><strong>SIP</strong>&lt;br&gt;Specifies the SIP request method or response code. <strong>H.323</strong>&lt;br&gt;Identifies the registration request, reject, or confirm messages.</td>
</tr>
<tr>
<td></td>
<td>Details</td>
<td>The text of the event message.</td>
</tr>
<tr>
<td>Registration end</td>
<td>Reason</td>
<td>Specifies if the registration event was terminated by the remote endpoint or by the RealPresence DMA system.</td>
</tr>
</tbody>
</table>

#### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TURN Status</td>
<td>The status of the TURN server (Running or Stopped)</td>
</tr>
<tr>
<td>ID</td>
<td>Automatically generated ID for each TURN allocation</td>
</tr>
<tr>
<td>User</td>
<td>The username of the WebRTC client that requested the allocation</td>
</tr>
<tr>
<td>Realm</td>
<td>The realm used to authenticate the allocation</td>
</tr>
<tr>
<td>Client Address</td>
<td>The WebRTC client's public IP address</td>
</tr>
<tr>
<td>Relay Address</td>
<td>The public IP address for TURN media relay, mapped on the firewall (the <strong>External IP Address of NAT</strong>)</td>
</tr>
<tr>
<td>Server Address</td>
<td>The public IP address of either the client that requested the allocation or the peer, depending on the direction of media relay.</td>
</tr>
<tr>
<td>Age (seconds)</td>
<td>The number of seconds that the allocation has been active</td>
</tr>
<tr>
<td>Expires (seconds)</td>
<td>The number of seconds remaining until the allocation expires if it is not renewed by the client</td>
</tr>
</tbody>
</table>
3. Click the down arrow next to the Refresh button and select a refresh interval.
The allocation details refresh based on the interval you select.

Manage 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 Configure Log Settings.

These topics provide details on working with system log files:

- View the Disposition for SIP and H.323 Calls
- Download Log Files
- Delete Log Files
- Roll Log Files

View the Disposition for SIP and H.323 Calls

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

The following tables describe the different dispositions.

### SIP Dispositions

<table>
<thead>
<tr>
<th>Disposition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>RealPresence Access Director system license controller and SIP module accepts a new SIP call</td>
</tr>
<tr>
<td>Forward</td>
<td>RealPresence Access Director system SIP module forwards a SIP request/response</td>
</tr>
<tr>
<td>Reject</td>
<td>RealPresence Access Director system SIP module rejects a SIP call</td>
</tr>
<tr>
<td>Discard</td>
<td>RealPresence Access Director system SIP module discards a SIP request/response</td>
</tr>
<tr>
<td>Release</td>
<td>RealPresence Access Director system SIP module releases a SIP call session</td>
</tr>
</tbody>
</table>
H.323 Dispositions

<table>
<thead>
<tr>
<th>Disposition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>RealPresence Access Director system H.323 module forwards an H.323 message</td>
</tr>
<tr>
<td>Auto-response</td>
<td>RealPresence Access Director system H.323 module automatically responds</td>
</tr>
<tr>
<td>Auto-request</td>
<td>RealPresence Access Director system H.323 module automatically sends a request</td>
</tr>
<tr>
<td>Release</td>
<td>RealPresence Access Director system H.323 module releases an H.323 call session</td>
</tr>
</tbody>
</table>

Download Log Files

From the System Log Files page, you can select log files to download.

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.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Date and time that the log file was created.</td>
</tr>
<tr>
<td>Host</td>
<td>Host name of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>Filename</td>
<td>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.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the file in megabytes.</td>
</tr>
</tbody>
</table>

To download a system log file:

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

Delete Log Files

You can delete log files when they are no longer needed.
To delete a system log file:

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

Roll Log Files

Use the Roll Logs action to convert an active log file into an archive file.

To roll an active log file into an archive file:

1. Go to Diagnostics > System Log Files.
2. Select the log file to roll.
4. A message displays to confirm that the rolled log file was created in the archive directory.
5. Click Yes to download the log file.
6. In the Save As dialog, select a location, and choose Save.
7. Click Close when the download is complete.

Run Traffic Capture

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

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

The maximum size of each packet capture file is 10 MB. If a capture is larger than 10 MB, the system creates additional files as needed (10 MB each). The system will create a maximum of 10 .pcap files, whether for one or multiple traffic captures. When the tenth file reaches 10 MB, the system overwrites the first .pcap file.

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

To run traffic capture:

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

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

To download a packet capture file:

1  Go to Diagnostics > System Log Files and select the .pcap file to download.
2  Under Actions, click Download Logs and select a location to save the file.
   The system notifies you when the download is complete.

Ping a Device

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

To run Ping on a network device:

1  Go to Diagnostics > Ping.
2  Enter an IP address or host name and click Ping.
   The system displays the results of the command.

Run Traceroute

Use Traceroute to view these details:

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

To run Traceroute on an address:

1  Go to Diagnostics > Traceroute.
2  Enter an IP address or host name and click Trace.
   The system displays the results of the command.

View High Availability Status

The High Availability Status page provides details about various components of High Availability, including the following:

- Local and peer connection status
- Virtual IP addresses (active/inactive, owner, plumbed status)
- Interface and HA link status

To view status details for High Availability:

1  Go to Diagnostics > High Availability Status.
2  Click Refresh as need to update the information.

Use Polycom Utilities

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

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

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

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

- Remote Client Login 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 System
- Cannot Open RealPresence Access Director System User Interface

For additional information on troubleshooting, see Polycom Unified Communications in RealPresence Access Director System Environments, available at support.polycom.com.
## Remote Client Login Failed

<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| Access proxy error       | **In the RealPresence Access Director system:**  
  • Go to the **Services Status** pane on the Dashboard and check whether access proxy is running. If it has stopped running, complete the following steps:  
  **In the RealPresence Resource Manager system**  
  • Do one of the following:  
    ▶ Check whether the RealPresence Access Director system is accessible.  
  **On the inside firewall:**  
  • Check the firewall policy to determine if the HTTPS, LDAP, and XMPP ports all permit calls from the untrust to trust zone. Default values are:  
    ▶ HTTPS: TCP 443  
    ▶ LDAP: TCP 389  
    ▶ XMPP: TCP 5222  
  **In the RealPresence Access Director system:**  
  • Wait 10 minutes, then check whether access proxy is running.  
  • Restart the system if access proxy is still not running. |
| Firewall configuration error | **On the outside firewall:**  
  • Check whether the public IP address of the RealPresence Access Director system is mapped to its internal signaling IP address.  
  • Check the firewall policy to determine if HTTPS, LDAP and XMPP ports are all permitted from untrust to trust zone. Default values are:  
    ▶ HTTPS: TCP 443  
    ▶ LDAP: TCP 389  
    ▶ XMPP: TCP 5222 |
| Certificate check fails  | **In the RealPresence Access Director system:**  
  • Go to **Configuration > Access Proxy Settings**.  
  • Select **HTTPS_proxy** 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. |
### Possible Reasons | Recommended Actions
--- | ---
No network connection on Polycom® RealPresence® Mobile | Check the wireless connection on the mobile device.
Sign-in server address error | Confirm that the sign-in server address for the remote user, is the public address of the RealPresence Access Director system.
Site configuration error | In the RealPresence Resource Manager system, check whether the signaling IP address of the RealPresence Access Director system is included in the subnets.
User configuration error | In the RealPresence Resource Manager system, check whether the user that is signed in can be found in a search of the local user list or in the LDAP user list.

**Licensed Call Number is 0**

| Possible Reasons | Recommend Actions |
--- | --- |
Trial period expires | Purchase a license. In the RealPresence Access Director system:
  • Go to Maintenance > License > Activation Keys and enter the new key.
  • Click Update. |
License is invalid due to system time being changed. | If you have purchased a license, in the RealPresence Access Director system:
  • Go to Maintenance > License > Activation Keys and re-enter the license activation key.
  • Click Update. |

**SIP Registration Failed**

| Possible Reasons | Recommend Actions |
--- | --- |
SIP component not running | In the RealPresence Access Director system:
  • Go to the Services Status pane on the Dashboard and check whether SIP services are running. If not, complete the following steps:
  • Go to Configuration > SIP Settings.
  • Check whether SIP is enabled. If not, select Enable SIP signaling.
  • Check the Services Status pane again to see if SIP services are running. If not, restart the system. |
<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP configuration error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to Configuration &gt; SIP Settings.</td>
</tr>
<tr>
<td></td>
<td>• Check the value of Registration refresh interval.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the system listens on the same SIP port and for the same transport protocol that the registered endpoint uses.</td>
</tr>
<tr>
<td></td>
<td>In the RealPresence DMA system:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the Minimum SIP registration interval of the SIP registrar server allows the registration refresh interval from the RealPresence Access Director system.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the SIP registrar server listens on the configured SIP port and protocol used by the RealPresence Access Director system.</td>
</tr>
<tr>
<td>SIP server address error</td>
<td>On the remote endpoint:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the SIP registrar server address is the public address of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>TLS port error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to Configuration &gt; SIP Settings.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the TLS port is 5061, not 5060, for communication between the RealPresence Access Director system and the RealPresence DMA system.</td>
</tr>
<tr>
<td>Site configuration error</td>
<td>In the RealPresence Resource Manager system, check whether the SIP registrar server address for remote users is the public address of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>Authentication error</td>
<td>In the RealPresence DMA system:</td>
</tr>
<tr>
<td></td>
<td>• Go to Admin &gt; Local Cluster &gt; Signaling Settings &gt; SIP Settings.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the SIP registrar server enables SIP authentication and ensure that the client uses the correct SIP account.</td>
</tr>
<tr>
<td>Firewall configuration error</td>
<td>In the RealPresence DMA system:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the RealPresence Access Director system is accessible.</td>
</tr>
<tr>
<td></td>
<td>On the inside firewall:</td>
</tr>
<tr>
<td></td>
<td>• Check the firewall policy to determine if SIP ports are all permitted from the untrust to trust zone. Default values are:</td>
</tr>
<tr>
<td></td>
<td>▲ TCP: 5060, 5061</td>
</tr>
<tr>
<td></td>
<td>▲ UDP: 5060</td>
</tr>
<tr>
<td></td>
<td>On the outside firewall:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the public signaling IP address of the RealPresence Access Director system is mapped to its internal signaling IP address.</td>
</tr>
<tr>
<td></td>
<td>• On both the outside and inside firewalls, check the firewall policy to determine if SIP ports are permitted from the untrust to trust zone.</td>
</tr>
<tr>
<td>Possible Reasons</td>
<td>Recommend Actions</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificate installation error</td>
<td>If the client uses SIP TLS, check whether the certificates on the RealPresence Access Director system are correctly installed. <strong>Note:</strong> The RealPresence Access Director system does not support PKCS #12 certificates.</td>
</tr>
<tr>
<td><strong>SIP Call Failed</strong></td>
<td></td>
</tr>
<tr>
<td>Possible Reasons</td>
<td>Recommend Actions</td>
</tr>
</tbody>
</table>
| Endpoint registration error             | On the caller and callee endpoints:  
  • Check whether both endpoints are registered.  
  • Unregister and reregister the endpoints and call again.                                                                                                                                                                                                                                                   |
| Service network setting error           | In the RealPresence Access Director system:  
  • Go to **Admin > Network Settings**.  
  • Review the **Service network settings**.  
  • If the RealPresence Access Director system is deployed behind the outside firewall, check the **NAT Settings** to ensure the following:  
    ▲ **Deployed behind Outside Firewall with NAT** is selected.  
    ▲ **Signaling Relay Address** and **Media Relay Address** specify the public signaling IP address and the public media IP address of the RealPresence Access Director system mapped on the outside firewall. |
| License limitation                      | In the RealPresence Access Director system:  
  • Go to the **License Status** pane on the Dashboard.  
  • Check whether the **Maximum Allowed Calls** have been reached.                                                                                                                                                                                                                                           |
| RealPresence DMA system configuration   | In the RealPresence DMA system, determine if the dial rule configurations are correct.                                                                                                                                                                                                                     |
| error                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SIP ALG                                 | • Check whether SIP ALG is enabled on the firewall/NAT.  
  • If enabled, disable SIP ALG and try the call again.                                                                                                                                                                                                                                                         |
| Bandwidth limitation                    | Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system. When this happens, complete the following steps:  
  • Go to **Configuration > Media Traversal Settings**.  
  • Increase bandwidth limitation values.  
  • Try the call again.                                                                                                                                                                                                                               |
# H.323 Call Failed

<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 component not running</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to the <strong>Services Status</strong> pane on the Dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Check whether H.323 is running. If not, complete the following steps:</td>
</tr>
<tr>
<td></td>
<td>‣ Go to <strong>Configuration &gt; H.323 Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>‣ Check whether H.323 signaling is enabled. If not, select <strong>Enable H.323 signaling</strong>.</td>
</tr>
<tr>
<td></td>
<td>‣ Restart the system if H.323 is still not running.</td>
</tr>
<tr>
<td>Callee registration error</td>
<td>On the callee endpoint, check whether the endpoint is registered with the gatekeeper.</td>
</tr>
<tr>
<td>H.323 configuration error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to <strong>Admin &gt; Network Settings &gt; Service network setting</strong>.</td>
</tr>
<tr>
<td></td>
<td>• If the RealPresence Access Director system is deployed behind an outside firewall, check the <strong>NAT Settings</strong> to ensure the following:</td>
</tr>
<tr>
<td></td>
<td>‣ <strong>Deployed behind Outside Firewall with NAT</strong> is selected.</td>
</tr>
<tr>
<td></td>
<td>‣ <strong>Signaling Relay Address</strong> and <strong>Media Relay Address</strong> specify the public signaling IP address and the public media IP address of the RealPresence Access Director system mapped on the outside firewall.</td>
</tr>
<tr>
<td></td>
<td>• Go to <strong>Configuration &gt; H.323 Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that all RealPresence DMA system and internal endpoint subnets are included as CIDR addresses.</td>
</tr>
<tr>
<td>License limitation</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to the <strong>License Status</strong> pane on the Dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the <strong>Maximum Allowed Calls</strong> have been reached.</td>
</tr>
<tr>
<td>Network issue between the RealPresence Access Director system and the gatekeeper</td>
<td>In the RealPresence DMA system, check whether the RealPresence Access Director system is reachable.</td>
</tr>
<tr>
<td>H.225 port error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to <strong>Configuration &gt; H.323 Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the RealPresence Access Director system and the endpoint use the same H.225 signaling port, which is 1720 by default.</td>
</tr>
<tr>
<td>Firewall configuration error</td>
<td>On the outside firewall:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the public signaling IP address of the RealPresence Access Director system is mapped to its internal IP address.</td>
</tr>
<tr>
<td></td>
<td>On the outside and inside firewall</td>
</tr>
<tr>
<td></td>
<td>• Check the firewall policy to determine if H.323 ports are permitted from the untrust to trust zone.</td>
</tr>
<tr>
<td></td>
<td>‣ Default H.323 port is 1720.</td>
</tr>
<tr>
<td>Possible Reasons</td>
<td>Recommend Actions</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RealPresence DMA system configuration error</td>
<td>In the RealPresence DMA system, determine if the dial rule configurations are correct.</td>
</tr>
<tr>
<td>H.323 ALG</td>
<td>• Check whether H.323 ALG is enabled on the firewall/NAT.</td>
</tr>
<tr>
<td></td>
<td>• Disable H.323 ALG and try the call again.</td>
</tr>
<tr>
<td>Bandwidth limitation</td>
<td>Concurrent calls may reach the maximum bandwidth allowed by the RealPresence Access Director system. When this happens, complete the following steps:</td>
</tr>
<tr>
<td></td>
<td>• Go to Configuration &gt; Media Traversal Settings.</td>
</tr>
<tr>
<td></td>
<td>• Increase bandwidth limitation values.</td>
</tr>
<tr>
<td></td>
<td>• Try the call again.</td>
</tr>
</tbody>
</table>

**VMR Call Failed**

<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call signaling error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Check whether a SIP or H.323 peer-to-peer call works correctly.</td>
</tr>
<tr>
<td></td>
<td>▲ If so, the RealPresence Access Director system, the RealPresence DMA system, the endpoint, and the firewall configurations are all correct.</td>
</tr>
<tr>
<td></td>
<td>▲ If a peer-to-peer call does not work correctly, see the possible reasons in SIP Call Failed and H.323 Call Failed.</td>
</tr>
<tr>
<td>VMR configuration error</td>
<td>In the RealPresence DMA system, determine if the VMR number is correct.</td>
</tr>
<tr>
<td>RealPresence DMA system configuration error</td>
<td>In the RealPresence DMA system, determine if the dial rule configurations are correct.</td>
</tr>
</tbody>
</table>

**No Audio, Video, or Content**

<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media relay component error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to the Services Status pane on the Dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the Media Relay is running.</td>
</tr>
<tr>
<td></td>
<td>• Restart the system if Media Relay stops working.</td>
</tr>
<tr>
<td>Endpoint error</td>
<td>On the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• Check whether the audio is muted.</td>
</tr>
<tr>
<td></td>
<td>• Check whether the camera works correctly.</td>
</tr>
</tbody>
</table>
### Possible Reasons | Recommend Actions
--- | ---
Service network setting | In the RealPresence Access Director system:
- Go to **Admin > Network Settings > Service network setting**.
- If the RealPresence Access Director system is deployed behind an outside firewall, check the **NAT Settings** to ensure the following:
  - **Deployed behind Outside Firewall with NAT** is selected.
  - **Signaling Relay Address** and **Media Relay Address** specify the public signaling IP address and the public media IP address of the RealPresence Access Director system mapped on the outside firewall.

BFCP over UDP for content | The RealPresence Access Director system supports BFCP over UDP. Make sure the endpoint or MCU supports BFCP over UDP as well.

SIP or H.323 ALG | **Check whether SIP or H.323 ALG is enabled on the firewall/NAT.**
  - Disable SIP or H.323 ALG and try the call again.

Firewall configuration error | On the outside firewall:
- Check the firewall policy to determine if external media ports are permitted from an untrust to trust zone.
  - UDP: 20001–40000

| On the inside firewall:
- Check the firewall policy to determine if internal media ports are permitted from an trust to untrust zone.
  - UDP: 40001–60000

---

**Failed to Connect to RealPresence Resource Manager System**

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

Network issue between the RealPresence Access Director system and the RealPresence Resource Manager system | In the RealPresence Resource Manager system, check whether the RealPresence Access Director system is accessible.

Certificate check fails | In the RealPresence Access Director system:
- Go to **Admin > Polycom Management System**.
- Check whether **Verify certificate from internal server** is selected.
  - If selected, disable the field and try the call again.
<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate install error</td>
<td>In the RealPresence Access Director system:</td>
</tr>
<tr>
<td></td>
<td>• Go to Admin &gt; Polycom Management System.</td>
</tr>
<tr>
<td></td>
<td>• Check whether Verify certificate from internal server is selected.</td>
</tr>
<tr>
<td></td>
<td>• If selected, check whether the certificates on the RealPresence Access Director system and the RealPresence Resource Manager system are correctly installed.</td>
</tr>
<tr>
<td>Site configuration error</td>
<td>• In the RealPresence Resource Manager system, ensure that the subnet of the internal signaling IP address of the RealPresence Access Director system is correct.</td>
</tr>
<tr>
<td>User configuration error</td>
<td>In the RealPresence Resource Manager system, check whether the login name of the user is in the user list.</td>
</tr>
</tbody>
</table>

**Cannot Open RealPresence Access Director System User Interface**

<table>
<thead>
<tr>
<th>Possible Reasons</th>
<th>Recommend Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer browser cache issue</td>
<td>• Close and re-open the Internet Explorer browser.</td>
</tr>
<tr>
<td></td>
<td>• Access the RealPresence Access Director system user interface. If you are still unable to open the interface, delete the Internet Explorer cache files.</td>
</tr>
<tr>
<td></td>
<td>• Refer to Internet Explorer or Windows help if you do not have the necessary account permissions to delete the cache files.</td>
</tr>
</tbody>
</table>