# Contents

## Conventions Used in This Guide
- 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

## Unified Communications with the Polycom® RealPresence® Access Director™ Solution ............................................ 12
- Overview of the Polycom RealPresence Access Director Solution .............................................. 12
- RealPresence Access Director System Solution Deployment Models ........................................... 15
  - Deployment with One Firewall and a Single Network Interface .............................................. 15
  - Deployment in a DMZ NAT Environment with One or More Network Interfaces ......................... 15
  - Deployment in a Two-System Tunnel Configuration ................................................................. 16
  - Deployment with High Availability ......................................................................................... 17
  - Other Deployment Models ................................................................................................. 17
  - Integration with an F5 Load Balancer .................................................................................. 18
- Supported Call Scenarios .................................................. 18
  - Remote User Connections (SIP and H.323) ................................................................. 18
  - Guest User Connections (SIP and H.323) ........................................................................ 18
  - Federated or Neighbored Trust Connections (SIP and H.323) ............................................. 19
  - WebRTC Browser-Based Connections ............................................................................. 19
- Products Supported in this Solution ........................................ 19

## Deploying the RealPresence Access Director System in a Corporate DMZ Environment ........................................ 22
- Configure the DNS Service .................................................... 23
Task 1: Create DNS A and PTR records on the external DNS server ............. 23
Task 2: Create a DNS SRV record on the external DNS server ............... 24
Task 3: Create DNS A and PTR records on the internal DNS server .......... 24
Task 4: Create DNS SRV records on the internal DNS server ............... 25
Task 5: Create DNS A records for STUN and TURN services .............. 25
Task 6: Validate DNS settings on the external DNS server ..................... 27
Task 7: Validate DNS settings on the internal DNS server ...................... 27

Configure Firewalls and Ports ..................................................... 27
Firewalls with SIP/H.323 ALG .................................................. 28
Outside Firewall Configuration .................................................. 28
Inside Firewall Configuration ................................................... 28
Port Mapping ................................................................. 29

Install and Configure the RealPresence Access Director System .............. 29
Task 1: Perform Basic Installation ............................................ 29
Task 2: Configure Time Settings .............................................. 29
Task 3: Activate the License .................................................... 31
Appliance Edition ............................................................. 31
Virtual Edition ................................................................. 31
Task 4: Configure Network Settings ......................................... 32

Configure the RealPresence Resource Manager System .......................... 33

Configure the RealPresence Access Director System ............................. 34
Task 1: Configure Access Proxy Settings .................................... 35
Task 2: Configure Basic Access Control List Settings ......................... 35
Task 3: Configure System Certificates ..................................... 36
Task 4: Configure TURN Services ........................................... 36
Task 5: Provision the RealPresence Access Director System ................ 37

Configure the Polycom RealPresence DMA System .............................. 37
Task 1: Enable SIP Device Authentication .................................. 37
Task 2: Configure an External SIP Peer to Support SIP Open B2B Calls ... 38
Task 3: Configure SIP Settings for Guest Users ............................... 39
   SIP Settings for Guest Users on the Polycom DMA System ........... 40
   SIP Settings for Guest Users on the RealPresence Access Director System ... 40
Task 4: Configure SIP Settings for Remote Users .............................. 41
   SIP Settings for Remote Users on the RealPresence Access Director System ... 41

Configure Polycom Endpoint Systems ............................................. 41
Task 1: Configure Polycom HDX Series Endpoints ............................... 41
Task 2: Configure the Polycom Group Series System ....................... 41
Task 3: Configure Polycom RealPresence Mobile or Desktop Endpoints ... 42
   Professional Mode Sign-In Settings ..................................... 42
Configure the Polycom RealPresence Collaboration Server ..................... 42
Deploying Two RealPresence Access Director Systems in a Tunnel Configuration

Configure the DNS Service for the Two-System Tunnel
Configure Firewalls and Ports
  Outside Firewall Configuration
  Inside Firewall Configuration
Install and Configure the RealPresence Access Director Systems
  Task 1: Perform Basic Installation
  Task 2: Synchronize the Time and Set the Time Zones
  Task 3: Activate the System Licenses for Appliance Edition Servers
  Task 4: Configure Network Settings for the Tunnel Server
  Task 5: Configure Network Settings for the Tunnel Client
  Task 6: Configure Two-Box Tunnel Settings on the Tunnel Server
  Task 7: Configure Two-Box Tunnel Settings on the Tunnel Client
  Task 8: Configure System Certificates
  Task 9: Configure Access Control List Rules and Rule Settings
Configure the RealPresence Resource Manager System
Configure the Polycom RealPresence DMA System
Configure Additional Polycom Components

Deploying RealPresence Access Director Systems with High Availability

High Availability Overview
  Failovers
Network Settings to Support High Availability
  Network Interface Configuration Options
Configure Network Settings
High Availability Requirements
Configure High Availability Settings
  Change HA Password
Firewall Configuration
  Option 1: Two Public IP Addresses (NAT Required)
  Option 2: Four Public IP Addresses (NAT not Required)
High Availability Status
Log Files
  View Log Files
Licensing
Federation Between RealPresence Access Director Systems .......................... 66
Federation in a SIP Environment ............................................................. 66
  Task 1: Create Additional DNS SRV Records on the External DNS Server .... 66
  Task 2: Obtain and Install the Certificates for the RealPresence Access Director Systems . 67
  Task 3: Configure the RealPresence Access Director Systems to Support Federated SIP Calls .......................................................... 67
  Task 4: Configure the Polycom RealPresence DMA Systems to Support Federated SIP Calls 68
Federation in an H.323 Environment ......................................................... 69
  Task 1: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls ....................................................... 69
  Task 2: Configure the Polycom RealPresence DMA Systems to Support Federated H.323 Calls .............................................................. 70
Federation Between RealPresence Access Director and Other Systems ......... 71
Federation in an H.323 Environment with Polycom VBP-E Systems .............. 71
  Task 1: Create an Additional DNS A Record on the External DNS Server .... 71
  Task 2: Create Additional DNS SRV Records on the External DNS Server .... 72
  Task 3: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls ....................................................... 72
  Task 4: Configure the Polycom RealPresence DMA System to Support Federated H.323 Calls .............................................................. 73
  Task 5 (Conditional): Configure the CMA System to Support Federated H.323 Calls . 73
  Task 6 (Conditional): Configure the VBP-5300E System to Support Federated H.323 Calls . 74
  Task 7 (Conditional): Configure the VBP-5300E System in Embedded Gatekeeper Mode to Support Federated H.323 Calls ......... 74
Federation in a SIP Environment with Acme Packet .................................. 74
Verifying Deployment ................................................................................. 75
  Verifying Access Proxy ........................................................................ 75
  Verifying Call Success ......................................................................... 75
  Verifying Certificates ......................................................................... 75
Required Ports .......................................................................................... 77
  Management Access ........................................................................... 78
  Management Access Ports ................................................................. 78
  SIP Signaling ...................................................................................... 81
SIP WAN Ports ............................................ 82
SIP LAN Ports ............................................ 83
H.323 Signaling ............................................ 84
  H.323 WAN Ports ........................................ 84
  H.323 LAN Ports ........................................ 85
Access Proxy ............................................. 87
  Access Proxy WAN Ports ............................... 88
  Access Proxy LAN Ports ............................... 91
Media ..................................................... 92
  Media WAN Ports ....................................... 92
  Media LAN Ports ....................................... 93
TURN Server ............................................. 93
  TURN Relay Ports ..................................... 94
High Availability ....................................... 95
  Two-System Tunnel Communication ................ 95
Comparison of Two-box Tunnel Deployment and Standard Deployment Ports ....... 96

Network Interface Configurations ............................................. 98
  Single Firewall Deployment with One Network Interface .................. 98
  DMZ Deployment with One or More Network Interfaces .................. 99
    Standard Configuration .................................. 99
    LAN-WAN Configuration ................................ 100
  Two-System Tunnel Deployment .................................. 101
    Tunnel Server Network Interface Configuration .................. 102
    Tunnel Client Network Interface Configuration .................. 102
  High Availability Deployment .................................. 103
Conventions Used in This Guide

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.

<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><em>Italics</em></td>
<td>Used to emphasize text, to show example values or inputs (in this form: <em>&lt;example&gt;</em>), 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

This guide describes the Polycom® RealPresence® Access Director™ solution and the process of deploying the products in the solution. The solution provides firewall traversal for the connections required for the supported deployment architecture, models, and user scenarios.

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 specific — that is, RealPresence Access Director, Virtual Edition or RealPresence Access Director, Appliance Edition.

Audience, Purpose, and Required Skills

This content is written for a technical audience. Integrating Polycom infrastructure and endpoint systems with the RealPresence Access Director system requires planning and elementary knowledge of Polycom video conferencing and video conferencing administration.

This is not a training document. Polycom assumes those deploying this solution have a solid understanding of networking, firewalls, Network Address Translation (NAT), Domain Name Systems (DNS), H.323, and SIP concepts.

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 System Getting Started Guide
- Polycom RealPresence Access Director System Administrator Guide
- Polycom RealPresence Platform Director System Administrator Guide

In addition, you will need the product documentation for the other infrastructure products required for this solution, including:

- Polycom RealPresence DMA System Operations Guide
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.
Unified Communications with the Polycom® RealPresence® Access Director™ Solution

In this solution, Polycom’s integrated suite of video conferencing systems includes the RealPresence Access Director system, which:

- Secures the borders to the enterprise IP network, the private VPN, and the Internet for video collaboration within and beyond the firewall.
- Enables high-quality and secure unified communications between divisions or enterprises, remote users, and guest users.
- Combines remote, guest, open, and B2B calling scenarios with SIP and H.323 (AVC and SVC) capabilities.
- Provides secure scalability for a mobile workforce.

The following topics describe the Polycom solution that includes the RealPresence Access Director system as the session border controller (SBC) for a site’s IP network.

- Overview of the Polycom RealPresence Access Director Solution
- RealPresence Access Director System Solution Deployment Models
- Supported Call Scenarios
- Products Supported in this Solution

Overview of the Polycom RealPresence Access Director Solution

The Polycom video infrastructure integrates with the RealPresence Access Director system to provide video conferencing management for remote, guest, federated, and unfederated users with secure firewall traversal for all of the required connections. The following table describes the network traversal services this solution secures.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Access Proxy</td>
<td>Enables remote and guest users via designated video endpoints to make HTTPS connections to the RealPresence Access Director system, which are then proxied to the internal Polycom® RealPresence® Resource Manager system, the RealPresence Content Sharing Suite, and other HTTPS application servers, including the Polycom® RealPresence® CloudAXIS™ Suite Experience Portal (MEA) and the RealPresence CloudAXIS Services Portal (WSP).</td>
</tr>
<tr>
<td>XMPP Access Proxy</td>
<td>Enables XMPP signaling from remote users via designated video endpoints to traverse the firewall to the internal XMPP servers you specify in configuration settings. XMPP access proxy also enables sending of outgoing XMPP signaling to remote endpoints.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDAP Access Proxy</td>
<td>Enables remote and guest users via designated video endpoints to make LDAP connections to the RealPresence Access Director system, which are then proxied to the internal LDAP servers you specify in configuration settings. used by the RealPresence Resource Manager system, or other LDAP application servers.</td>
</tr>
<tr>
<td>HTTP Tunnel Proxy</td>
<td>An HTTP tunnel proxy enables CloudAXIS suite SIP guest users to attend video conferences in your enterprise’s CloudAXIS suite Experience Portal. Some restrictive networks block outgoing UDP-based traffic and can limit outgoing TCP traffic to ports 80 and 443. In these situations, if a CloudAXIS suite SIP guest cannot establish a native SIP/RTP connection to a 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 guest 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)/TCP content.</td>
</tr>
<tr>
<td>SIP Signaling</td>
<td>Enables:</td>
</tr>
<tr>
<td></td>
<td>• Firewall traversal for SIP traffic from remote and guest users with supported video endpoints to the internal SIP server.</td>
</tr>
<tr>
<td></td>
<td>• SIP open business-to-business (B2B) calling, which supports calls from external SIP endpoints that are not registered or are not members of a federated enterprise or division.</td>
</tr>
<tr>
<td></td>
<td>• Outbound SIP signaling to registered, guest and open B2B endpoints.</td>
</tr>
<tr>
<td></td>
<td>• Use of separate interfaces for external and internal SIP signaling traffic.</td>
</tr>
<tr>
<td></td>
<td>• Modifying SIP signaling to direct media through the media relay when required.</td>
</tr>
<tr>
<td>H.323 Signaling</td>
<td>Enables:</td>
</tr>
<tr>
<td></td>
<td>• Firewall traversal for H.323 traffic from remote and guest users with supported video endpoints to the internal gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>• H.323 open business-to-business (B2B) calling, which supports calls from external H.323 endpoints that are not registered or are not members of a neighbored enterprise or division.</td>
</tr>
<tr>
<td></td>
<td>• Outbound H.323 signaling to registered, guest and open B2B endpoints.</td>
</tr>
<tr>
<td></td>
<td>• Use of separate interfaces for external and internal H.323 signaling messages</td>
</tr>
<tr>
<td></td>
<td>• Functionality to understand and manipulate all H.323 Annex O dialing messages.</td>
</tr>
<tr>
<td></td>
<td>• Functionality to route all H.323 messages from guest users to and from the internal gatekeeper.</td>
</tr>
<tr>
<td>Media Relay</td>
<td>Enables firewall traversal for media to and from remote and guest users with supported video endpoints. The media relay functions as a Session Border Controller (SBC)-based relay.</td>
</tr>
<tr>
<td>Static Routing</td>
<td>Enables use of static routes to route traffic to the correct network destination. One or more static routes may be defined for each network interface.</td>
</tr>
<tr>
<td>H.460 Support</td>
<td>The RealPresence Access Director system enables videoconference participants with H.460-enabled endpoints to register to a Polycom® RealPresence® Distributed Media Application™ (RealPresence DMA™ system), which acts as an H.323 gatekeeper, and place and receive H.323 calls across firewalls/NATs.</td>
</tr>
</tbody>
</table>
The RealPresence Access Director system is available in an Appliance Edition, packaged with a system server for an appliance based infrastructure. It is also available in a Virtual Edition, packaged as software only for deployment in a virtualized data center. Both editions provide the same firewall traversal functionality and can be integrated with other Polycom RealPresence Platform components to provide a seamless video collaboration experience.

Virtual Editions of Polycom RealPresence Platform products such as the RealPresence Access Director system require the Polycom® RealPresence® Platform Director™ system to manage licensing of your products. Additionally, if your RealPresence Platform Director system is installed in a VMware® vCenter Server® environment with the required capacity, you can use the RealPresence Platform Director system to install Polycom software. You can also use your virtual environment tools to install product instances.
The Polycom® RealPresence® Platform Director™ system is included with all Virtual Edition products and is available at Polycom’s support site for download (support.polycom.com).

Before you install or upgrade your RealPresence Access Director system software, install the RealPresence Platform Director system and verify that your product is licensed.


RealPresence Access Director System Solution Deployment Models

The RealPresence Access Director system solution can be deployed based on several different models:

- Deployment with One Firewall and a Single Network Interface
- Deployment in a DMZ NAT Environment with One or More Network Interfaces
- Deployment in a Two-System Tunnel Configuration
- Deployment with High Availability
- Other Deployment Models

See Network Interface Configurations for diagrams of the deployment models and configuration details for the network interfaces.

Deployment with One Firewall and a Single Network Interface

In this simple model, the RealPresence Access Director system is deployed at the DMZ of the single firewall. All signaling, media, access proxy, and management traffic use one network interface and IP address.

Deployment in a DMZ NAT Environment with One or More Network Interfaces

In general, Polycom recommends that the RealPresence Access Director system be deployed in a corporate DMZ with Network Address Translation (NAT). This means that the system is deployed “back-to-back” between an outside IP address (also referred to as a public or external address) and an inside NATed address (also referred to as a private or internal address). Polycom Unified Communications with the RealPresence Access Director System Standard Deployment illustrates a standard deployment.
In a DMZ with NAT implementation:

- The outside firewall, which resides between the WAN (untrusted) and the RealPresence Access Director system, must be in Destination NAT mode. In this mode:
  - When inbound packets from the WAN pass through the firewall, it translates the destination IP address to that of the RealPresence Access Director system.
  - When outbound packets from the enterprise network pass through the firewall, it translates the source IP address to the outside IP address of the firewall system.
  - A static and direct 1:1 NAT mapping, with all required service ports and port ranges forwarded, is recommended for the outside firewall.

- The inside firewall, which resides between the RealPresence Access Director system and the LAN (trusted), must be in Route mode.
  - In this mode, the firewall does not change the destination or source IP address, so no translation is required or supported.

Deployment in a firewall/NATed environment takes advantage of the firewall’s security functionality. However, because all media and signaling traffic flows through the firewall, performance can be affected.

A RealPresence Access Director system that uses at least two network interfaces can be deployed in a LAN-WAN (“two-legged”) configuration. In this scenario, signaling and media traffic are split between the interfaces to separate external and internal traffic.

For details on how to configure the network interfaces, see DMZ Deployment with One or More Network Interfaces.

### Deployment in a Two-System Tunnel Configuration

Two RealPresence Access Director systems can be deployed in a tunnel configuration (see The RealPresence Access Director System Two-System Tunnel Deployment). In this model, one system acts
as the tunnel server and is deployed in the corporate back-to-back DMZ. The other system serves as a tunnel client and is deployed behind the inside firewall. Communication between the tunnel server and the tunnel client is through UDP transmission.

In a tunnel configuration, port mapping on the inside 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 is open and listening 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.

The RealPresence Access Director System Two-System Tunnel Deployment

![Diagram showing two systems with tunnel](image)

### Deployment with 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, which helps to ensure that users always have access to a RealPresence Access Director system within your network.

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 users 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.

See [Deploying RealPresence Access Director Systems with High Availability](#) for details.

### Other Deployment Models

If you have a three-legged firewall (one with at least three network interfaces), the same firewall can separate the RealPresence Access Director system in the DMZ from both the internal LAN and the Internet. Note that in this configuration, not all firewall traffic goes through the RealPresence Access Director system.

The three-legged firewall configuration requires a static and direct 1:1 NAT mapping between the WAN (untrust) and the DMZ, and Route mode between the DMZ and the LAN (trust).

[Network Interface Configurations](#) includes diagrams and the recommended network interface configurations supported for this solution.
Integration with an 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 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 according to the Round Robin algorithm. 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.

The configuration of the F5 load balancer’s routing policy must support persistence. Persistence ensures that all requests from the same source IP address during a session are distributed to the same RealPresence Access Director system. A heartbeat connection between the F5 load balancer and all RealPresence Access Director systems ensures that requests are routed only to an accessible system.

The F5 load balancer must be configured to integrate with your RealPresence Access Director systems, but no configuration is necessary on the RealPresence Access Director systems. See Integrate Two or More Systems with an F5 Load Balancer.

Supported Call Scenarios

The deployment models for this Polycom solution support the following user scenarios:

- Remote User Connections (SIP and H.323)
- Guest User Connections (SIP and H.323)
- Federated or Neighbored Trust Connections (SIP and H.323)
- WebRTC Browser-Based Connections

Remote User Connections (SIP and H.323)

A remote user is an enterprise user with a managed Polycom SIP or H.323 endpoint that lies outside of the enterprise network. In this user scenario:

- Remote users can participate in video calls with other enterprise users as if they were inside the enterprise network.
- Remote users can receive calls as if they were inside the network.
- Remote users can receive management services including endpoint provisioning, user directory, and XMPP contact list and presence services, as well as SIP and H.323 calling, calendaring, and scheduling services.

All RealPresence Access Director system deployment models support this user scenario.

Guest User Connections (SIP and H.323)

A guest user is a user with a non-managed SIP or H.323 endpoint that lies outside of the enterprise network. In this user scenario:

- Guest users can participate in video calls with division or enterprise users without being members of the enterprise network.
- Enterprise users can place H.323 calls out to guest users.
Enterprise users can place SIP calls out to guest users.

Guest users do not have access to any management services such as endpoint provisioning, user directory, XMPP contact list and presence services, or calendaring and scheduling services.

All RealPresence Access Director system deployment models support this user scenario.

**Federated or Neighbored Trust Connections (SIP and H.323)**

Enterprise users from one division or enterprise can call enterprise users from another division or enterprise when:

- Both division or enterprise users have supported and managed SIP or H.323 endpoints.
- Both division or enterprise sites have implemented a RealPresence Access Director system or other access solution for federation.
- The federated sites are connected by a mutually trusted connection. For SIP systems, this trust relationship is a SIP trunk. For H.323 systems, this trust relationship is mutually neighbored gatekeepers.
- The sites have established and supported dial plans.

In this user scenario, each user has access to their site’s provisioning, directory, presence, and calling services, as well as contact lists.

All RealPresence Access Director system deployment models support this user scenario. Additionally, you must complete the deployment processes described in the appropriate section for your deployment model:

- Federation Between RealPresence Access Director Systems
- Federation Between RealPresence Access Director and Other Systems

**WebRTC Browser-Based Connections**

Web Real-Time Communication (WebRTC) is a web-based technology that provides high-quality video and audio communication capabilities in some web browsers, without requiring installation of a custom plug-in. By using either Google Chrome or Mozilla Firefox, users both inside and outside your enterprise network can attend web-based Polycom® RealPresence® Web Suite Pro conferences, for which the RealPresence Access Director system relays media 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.

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

See the Polycom RealPresence Access Director System Administrator Guide for instructions on configuring TURN server settings and TURN users.

**Products Supported in this Solution**

See the Polycom RealPresence Access Director System Release Notes to view the products tested with your version of the system.
The following products are supported in the RealPresence Access Director system solution.

<table>
<thead>
<tr>
<th>Product</th>
<th>Function in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NAT, Firewall, Session Border Controllers</strong></td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Access Director</td>
<td>Provides secure access to H.323 and SIP video services for small- to medium-sized federated enterprises.</td>
</tr>
</tbody>
</table>

| **Management Systems and Recorders** | |
| Polycom RealPresence Resource Manager | Provisions and manages remote endpoints, and enables directory and presence services |
| Polycom RealPresence Content Sharing Suite and Polycom ContentConnect | Provide content sharing interoperability between Microsoft Lync 2010 and 2013 clients and Polycom video conferencing solutions |
| Microsoft Active Directory | Directory service that authenticates and authorizes all registered users and devices |

| **Gatekeepers, Gateways, and MCUs** | |
| Polycom RealPresence Collaboration Server (RMX) 1500, 2000, and 4000 | Provides bridge capability for SIP and H.323 conferences, including support for content over video |
| Polycom RealPresence Distributed Media Application (DMA) 7000 | Functions as SIP proxy/registrar, H.323 gatekeeper, SIP and H.323 gateway, and bridge virtualizer |

| **Endpoints** | |
| Polycom HDX 7000, 8000, and 9000 series | Video conferencing endpoint systems |
| Polycom RealPresence Mobile | Serves as client application for supported mobile devices |
| Polycom RealPresence Desktop | Serves as desktop client application |
| Polycom RealPresence Group Series 300/500 | Video conferencing endpoint systems |
| Cisco C20 Codec | Video conferencing endpoint system |
| Cisco C40 Codec | Video conferencing endpoint system |
| Cisco EX60 Desktop System | Video conferencing endpoint system |
| Cisco EX90 Desktop System | Video conferencing endpoint system |
| Cisco 1700 MXP Desktop System | Video conferencing endpoint system |

| **Web Browser-Based Solutions** | |
| Polycom RealPresence CloudAXIS Suite or Polycom RealPresence Web Suite | Provide two virtualized server components that enable users to schedule and participate in video conferences accessed from a web browser or other hardware and software video endpoints, including the Polycom RealPresence Mobile application. |
Polycom, Inc. RealPresence Platform Virtual Edition Infrastructure

<table>
<thead>
<tr>
<th>Product</th>
<th>Function in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Platform Director</td>
<td>Provides the ability to deploy, license, and monitor the RealPresence Platform, Virtual Edition products in an organization's data center or in the cloud.</td>
</tr>
</tbody>
</table>

Hypervisor Environments for Virtual Edition

<table>
<thead>
<tr>
<th>Hypervisor Environments for Virtual Edition</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
</tr>
<tr>
<td>Microsoft® Hyper-V</td>
</tr>
</tbody>
</table>
Deploying the RealPresence Access Director System in a Corporate DMZ Environment

This section describes the general configuration processes required for deploying the RealPresence Access Director system in a DMZ environment with one or more network interfaces. The chapters that follow describe additional configuration processes required for the specific deployment models.

The following cross-functional flow chart identifies the tasks you must perform.

See these topics for detailed information about each of the tasks:

- **Configure the DNS Service**
- **Configure Firewalls and Ports**
- **Install and Configure the RealPresence Access Director System**
- **Configure the RealPresence Resource Manager System**
Configure the RealPresence Access Director System

Configure the Polycom RealPresence DMA System

Configure Polycom Endpoint Systems

Configure the Polycom RealPresence Collaboration Server

Integrate Two or More Systems with an F5 Load Balancer

Configure the DNS Service

This section describes creating domain name system (DNS) records to enable this solution.

Task 1: Create DNS A and PTR records on the external DNS server

Create a DNS A (address) record and associated reverse PTR (pointer) record on the external DNS server. The A record maps the FQDN of the RealPresence Access Director system to its public IP address for signaling and access proxy. The PTR record for reverse lookup resolves the public IP address of the RealPresence Access Director to its FQDN.

- If the RealPresence Access Director system has the FQDN name `rpad.example.com`, add an A record as follows:
  
  `rpad.example.com IN A 192.168.11.175`

  Where:
  
  - FQDN = `rpad.example.com`
  - Class = `IN` (Internet)
  - A = Record type
  - `192.168.11.175` = RealPresence Access Director system public IP address for signaling and access proxy

- If your DNS management tool does not automatically create the PTR record that corresponds to the A record, add the PTR record manually as follows:

  ```
  175.11.168.192.in-addr.arpa.
  ```

  Where:
  
  - `175.11.168.192.in-addr.arpa.` = the RealPresence Access Director system IP address stored as the reverse DNS domain name, which points back to `rpad.example.com`.

If you have deployed Polycom ContentConnect™, RealPresence CloudAXIS Suite, or RealPresence Web Suite as part of your RealPresence Access Director solution, create a DNS A record and a PTR record on the external DNS server for the host(s) in those systems. The A records will resolve to the RealPresence Access Director system’s public IP address for signaling and access proxy; the PTR records will resolve to the RealPresence Access Director system’s FQDN.

Note: If necessary, get help with configuring the DNS records

If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.
Task 2: Create a DNS SRV record on the external DNS server

Create DNS service records (SRV records) on the external DNS server to map the SRV service addresses for dynamic endpoint provisioning, SIP registrar, and gatekeeper services to the FQDN of the RealPresence Access Director system.

If the RealPresence Access Director system has the FQDN name rpad.example.com, add these SRV records:

- `_cmaconfig._tcp.example.com IN SRV 0 100 443 rpad.example.com` (this SRV record is required by the Auto Find Provisioning Server feature of dynamically-managed endpoints.)
- `_sip._tcp.example.com IN SRV 0 100 5060 rpad.example.com`
- `_sip._udp.example.com IN SRV 0 100 5060 rpad.example.com`
- `_sip._tls.example.com IN SRV 0 100 5061 rpad.example.com` (optional*)
- `_sips._tcp.example.com IN SRV 0 100 5061 rpad.example.com`
- `_h323cs._tcp.example.com IN SRV 0 100 1720 rpad.example.com`
- `_h323ls._udp.example.com IN SRV 0 100 1719 rpad.example.com`

Where, for example:

- Service = `_sip`
- Protocol = `_tcp`
- Priority = 0
- Weight = 100
- Port = 5060
- Host offering this service = rpad.example.com

* The majority of products use `_sips._tcp`. However, to prevent call failures for the small percentage of devices that use `_sip._tls`, Polycom suggests that you also add the `_sip._tls` record.

Task 3: Create DNS A and PTR records on the internal DNS server

The RealPresence Access Director system, the RealPresence Resource Manager system, and the RealPresence DMA system in the internal network each need one A record on the internal DNS server to map their FQDNs to their respective IP addresses. Each system also needs a corresponding PTR record to resolve their IP addresses to their FQDNs. For example:

- If the FQDN of RealPresence Access Director system is `rpad.example.com`, and its IP address is `10.22.210.111`, create an A record:
  
  `rpad.example.com IN A 10.22.210.111`

- If the FQDN of RealPresence Resource Manager system is `rprm.example.com`, and its IP address is `10.22.202.134`, create an A record:
  
  `rprm.example.com IN A 10.22.202.134`

- If the FQDN of the RealPresence DMA system is `dma.example.com`, and its IP address is `10.22.120.126`, create an A record:
  
  `dma.example.com IN A 10.22.120.126`
Task 4: Create DNS SRV records on the internal DNS server

The RealPresence Resource Manager system requires a DNS SRV record on the internal DNS server to dynamically provision endpoints. The DNS SRV record maps the SRV service address to the FQDN of the RealPresence Resource Manager system.

- If the FQDN of the RealPresence Resource Manager system is `rprm.example.com`, and its IP address is `10.22.202.134`, create an SRV record as follows:

  `_cmaconfig._tcp.example.com IN SRV 0 100 443 rprm.example.com`

The RealPresence DMA system requires several DNS SRV records on the internal DNS server to map the SRV service address for SIP registrar and gatekeeper services to the FQDN of the RealPresence DMA system.

- If the FQDN of the RealPresence DMA system is `dma.example.com`, and its IP address is `10.22.120.126`, create these SRV records:

  `_sip._tcp.example.com IN SRV 0 100 5060 dma.example.com`
  `_sip._udp.example.com IN SRV 0 100 5060 dma.example.com`
  `_sip._tls.example.com IN SRV 0 100 5061 dma.example.com` *(optional*)
  `_sips._tcp.example.com IN SRV 0 100 5061 dma.example.com`
  `_h323cs._tcp.example.com IN SRV 0 100 1720 dma.example.com`
  `_h323ls._udp.example.com IN SRV 0 100 1719 dma.example.com`

* The majority of products use `_sips._tcp`. However, to prevent call failures for the small percentage of devices that use `_sip._tls`, Polycom suggests that you also add the `_sip._tls` record.

Task 5: Create DNS A records for STUN and TURN services

If you plan to enable STUN and TURN services on your RealPresence Access Director system, Polycom recommends that you create separate A records for these services on the external and internal DNS servers.

The A records on the external DNS server map the FQDNs of STUN and TURN to the public IP address for TURN services.

Create DNS A records on the external DNS server as follows:

- If the RealPresence Access Director system STUN service has the FQDN `stun.example.com`, add an A record as follows:

  `stun.example.com IN A 192.168.11.176`

Where:

- `FQDN = stun.example.com`
- `192.168.11.176 = RealPresence Access Director TURN service public IP address`
● If the RealPresence Access Director system TURN service has the FQDN `turn.example.com`, add an A record as follows:

```plaintext
turn.example.com IN A 192.168.11.176
```

Where:

- **FQDN** = `turn.example.com`
- **192.168.11.176** = RealPresence Access Director public IP address for TURN service

The A records on the internal DNS server map the FQDN of STUN to the public IP address for TURN service and the FQDN of TURN to the internal (private) IP address for TURN service.

Create DNS A records on the internal DNS server as follows:

- If the RealPresence Access Director system STUN service has the FQDN `stun.example.com`, add an A record as follows:

```plaintext
stun.example.com IN A 192.168.11.176
```

Where:

- **FQDN** = `stun.example.com`
- **192.168.11.176** = RealPresence Access Director public IP address for TURN service

- If the RealPresence Access Director system TURN service has the FQDN `turn.example.com`, add an A record as follows:

```plaintext
turn.example.com IN A 10.22.210.112
```

Where:

- **FQDN** = `turn.example.com`
- **10.22.210.112** = RealPresence Access Director internal (private) IP address for TURN service

The TURN A record on the internal DNS server should reference the internal IP address for TURN service.

The A record for TURN service on the internal DNS server should map the TURN FQDN to an internal IP address. Polycom recommends this configuration for a single network interface deployment and for LAN-WAN deployments where external and internal media relay services are assigned to separate interfaces.
Task 6: Validate DNS settings on the external DNS server

The following steps use the Windows `nslookup` commands as an example. The procedure is similar on Mac and Linux.

To validate the DNS settings on the external DNS server:

1. From a Windows computer located on the Internet network, open a command line.
2. Type `nslookup rpad.example.com` to check the A record of the RealPresence Access Director system. The response should include the corresponding RealPresence Access Director system's public IP address.
3. Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record. The response should include the FQDN of each RealPresence Access Director system.

Task 7: Validate DNS settings on the internal DNS server

The following steps use the Windows `nslookup` commands as an example. The procedure is similar on Mac and Linux.

To validate the DNS settings on the internal DNS server:

1. From a Windows computer located on the internal network, open a command line.
2. Type `nslookup rprm.example.com` to check the A record of the RealPresence Resource Manager system. The response should include the corresponding RealPresence Resource Manager system's IP address.
3. Type `nslookup dma.example.com` to check the A record of the RealPresence DMA system. The response should include the corresponding DMA system's IP address.
4. Type `nslookup rpad.example.com` to check the A record of the RealPresence Access Director system. The response should include the corresponding RealPresence Access Director system's internal IP address.
5. Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record of the RealPresence Resource Manager system. The response should include the FQDN of RealPresence Resource Manager system.
6. Type the following commands to check the SRV records of the RealPresence DMA system:
   
   `nslookup -type=srv _sip._tcp.example.com`
   `nslookup -type=srv _sip._udp.example.com`
   `nslookup -type=srv _sip._tls.example.com`
   `nslookup _sips._tcp.example.com`
   `nslookup _h323cs._tcp.example.com`
   `nslookup _h323ls._udp.example.com`

   Each response should include the FQDN of the RealPresence DMA system.

Configure Firewalls and Ports

For greater security, Polycom recommends that you disable SSH and web access connectivity from the Internet, and enable SSH and web access connectivity from the LAN.
Firewalls with SIP/H.323 ALG

Some firewalls and routers have SIP and H.323 ALG capabilities. These enable the firewall or router to identify, inspect, and sometimes modify the payload of SIP and H.323 traffic as it traverses the firewall or router. Modifying the payload helps the SIP or H.323 application from which the message originated to traverse NAT.

While many firewalls have perfectly operational SIP and H.323 ALG functions, they are generally limited in scope, and are not intended to properly handle complex, enterprise-grade needs. The following examples describe more complex implementations in which a SIP or H.323 ALG function on a router or firewall can cause problems with proper operation rather than assisting.

- Routed-mode gatekeeper services
- Multiple-session calls (for example, H.239/BFCP for content; far end camera control)
- Call encryption (TLS for SIP, Advanced Encryption Standard (AES) for H.323)
- Large capability-sets of modern video-conferencing devices, which cause SIP and H.323 communications to span multiple datagrams (H.323 H.245 terminal capability exchange, SIP Invite with SDP)
- Remote-firewall traversal techniques (H.460)

In addition to complex SIP and H.323 implementations, SIP and H.323 standards are in constant development. These factors make it unlikely that a firewall will meet all requirements to correctly perform ALG functions for SIP and H.323 traffic.

When you deploy the RealPresence Access Director system, you must disable all predefined services, such as SIP ALG and H.323 ALG, in your firewall. After these services are disabled, create port and protocol rules that use only source IP, destination IP, port, and transport protocol attributes (See Required Ports). When correct operation is confirmed without the predefined services, you can enable them according to your information security policy and work with your firewall vendor to resolve any performance issues.

Use the guidelines that follow to configure your firewalls and ports.

Outside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Configure 1:1 NAT
- Set interface mode to NAT
- Disable H.323 and SIP ALG (Application Layer Gateway)
- Disable any H.323 helper services on the firewall (for example, Cisco® H.323 Fixup).

Inside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Disable H.323 and SIP ALG
- Set interface mode to Route

Caution: If necessary, get help with firewall settings
If you’re not familiar with firewall concepts and administration and your enterprise’s firewall implementation, please consult with someone who is.
- Disable the port NAT.
- Disable any H.323 helper services on the firewall (for example, Cisco® H.323 Fixup).

**Port Mapping**

To enable firewall traversal for external clients, the RealPresence Access Director system uses ports for provisioning, presence, directory, call signaling, media, and content. The specific ports and port ranges configured 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.

Incoming traffic from external clients uses static ports you define in the RealPresence Access Director system user interface.

Outbound traffic from the RealPresence Access Director system uses dynamic source and destination ports from a range of port numbers (a port pool). The total number of ports available for use is based on the number of licensed calls on your system license. The RealPresence Access Director system automatically calculates dynamic port ranges based on your number of licensed calls. A port range for a specific function (for example, internal SIP signaling dynamic source ports) 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 do so, the RealPresence Access Director system will automatically calculate the end ranges.

See Required Ports for detailed port settings and refer to the Polycom RealPresence Access Director System Administrator Guide for instructions on configuring static ports and dynamic port ranges.

**Install and Configure the RealPresence Access Director System**

**Task 1: Perform Basic Installation**


Polycom RealPresence Platform products such as the RealPresence Access Director system, Virtual Edition require the RealPresence Platform Director system to deploy the software and to manage licensing. See the Polycom RealPresence Platform Director System Administrator Guide for detailed instructions on deploying the RealPresence Access Director system, Virtual Edition.

**Task 2: Configure 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, the Server Time (Refresh every 10 seconds) field displays the correct server time.

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

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

Consider the following information when configuring the time settings:

- You can configure up to three NTP server IP addresses from the RealPresence Platform Director system when you deploy an instance of the RealPresence Access Director system, Virtual Edition.
- Changing the time settings requires a system restart, which 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.
- 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, 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, TLS connections may fail.

**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.

**To configure the time settings:**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| System time zone                    | The time zone in which your RealPresence Access Director system is located.  
**Note:** After initial installation of the RealPresence Access Director system, the default time zone is GMT (UTC). You must select the time zone of your geographic location immediately after installation of the system. |
| Auto adjust for Daylight Saving Time | Automatically determined in accordance with the system time zone. If the system time zone you select observes Daylight Saving Time, this setting is enabled.  
**Note:** The administrator cannot change this setting. |
Task 3: Activate the License

Licenses for the Appliance Edition and Virtual Edition of the RealPresence Access Director system are managed differently. Refer to the following sections based on the edition you deployed.

Appliance Edition

To activate the license for your system, you must first obtain an activation key code from Polycom Support at support.Polycom.com. For instructions, see the Polycom RealPresence Access Director System Administrator Guide.

After you have an activation key code, you must activate the license from the RealPresence Access Director system, Appliance Edition web user interface.

To activate a license:

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

The system restarts.

Virtual Edition

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).


**Task 4: Configure Network Settings**

You must configure the network settings for the RealPresence Access Director system based on the deployment model you implement (see RealPresence Access Director System Solution Deployment Models). This section provides general network configuration instructions if you deploy one RealPresence Access Director system in your network DMZ. See the network settings information in the following chapters for instructions on other deployment models:

- Deploying Two RealPresence Access Director Systems in a Tunnel Configuration
- Deploying RealPresence Access Director Systems with High Availability

To configure the initial network settings for the RealPresence Access Director system follow the instructions in the Polycom RealPresence Access Director Getting Started Guide.

After you configure the initial network settings for the eth0 network interface, you can configure the settings for additional network interfaces as needed. For complete instructions, see the Polycom RealPresence Access Director System Administrator Guide.

To configure one or more 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 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:
   - 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 described in the following table:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP/H.323</td>
<td>• External signaling IP</td>
</tr>
<tr>
<td></td>
<td>• Internal signaling IP</td>
</tr>
<tr>
<td>Media Relay</td>
<td>• External relay IP</td>
</tr>
<tr>
<td></td>
<td>• Internal relay IP</td>
</tr>
</tbody>
</table>
Configure the RealPresence Resource Manager System

If you deploy your RealPresence Access Director system with a Polycom® RealPresence® Resource Manager system, the RealPresence Resource Manager system can provision some RealPresence Access Director system settings and dynamically manage (provision, upgrade, and manage) select remote endpoints.

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

The following table describes the settings that the RealPresence Resource Manager system can provision for 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>• <strong>External Access Proxy IP</strong>&lt;br&gt;From the <strong>Available IP address</strong> list, select an IP address and click the right arrow to move the IP address to the <strong>External Access Proxy IP</strong> list. You can select up to four interface IP addresses to act as external IP addresses for access proxy. See the chapter on <strong>Network Interface Configurations</strong> in <em>Deploying Polycom Unified Communications in RealPresence Access Director System Environments</em> for recommended settings based on the number of network interfaces.&lt;br&gt;• Internal Access Proxy IP&lt;br&gt;<strong>Note:</strong> You can assign one to four network interfaces as external access proxy IP addresses. Only one interface can be assigned as the internal access proxy IP address.</td>
</tr>
<tr>
<td>NAT</td>
<td>If <strong>Deployed behind Outside Firewall with NAT</strong> is enabled, complete these fields:&lt;br&gt;• Signaling relay address&lt;br&gt;• Media relay address</td>
</tr>
</tbody>
</table>

**Note:** Changing some network settings requires 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.

6 Click **Done > Commit and Reboot Now** to save the network settings.
The following list provides a high-level summary of the tasks you must complete to configure the RealPresence Resource Manager system to provision a RealPresence Access Director system and to provision endpoints that request provisioning through a RealPresence Access Director system. For detailed instructions, see The Polycom® RealPresence® Resource Manager System Operations Guide for your version of the RealPresence Resource Manager system.

- Create a site for the RealPresence Access Director system
  - If you deploy two RealPresence Access Director systems for High Availability, you need to create a separate site for each RealPresence Access Director system public IP address that maps to a virtual IP address. See Deploying RealPresence Access Director Systems with High Availability.
- Create a RealPresence Access Director system provisioning profile
- Create a network provisioning profile for endpoints
- Create a provisioning rule and associate it with all related profiles
- Create a user account for the RealPresence Access Director system

### Configure the RealPresence Access Director System

Once the RealPresence Resource Manager system has been configured to integrate with and provision the RealPresence Access Director system, you can finish configuring the RealPresence Access Director system, as described in the following tasks:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Server</td>
<td>Configures whether the RealPresence Access Director system uses a time server to synchronize system time.</td>
</tr>
<tr>
<td>Primary Time Server Address</td>
<td>The IP address of the primary time server that the system will use to synchronize time.</td>
</tr>
<tr>
<td>Secondary Time Server Address</td>
<td>The IP address of the secondary time server that the system will use to synchronize time.</td>
</tr>
<tr>
<td>Enable IP H.323</td>
<td>Configures the system to enable or disable H.323 call forwarding.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>The IP address of the internal gatekeeper to which the RealPresence Access Director system forwards gatekeeper registration or H.323 call requests from external endpoints.</td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Configures the system to enable or disable SIP call forwarding.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>The IP address of the internal SIP proxy server to which the RealPresence Access Director system forwards SIP calls from external endpoints. (This is the signaling IP address of the RealPresence DMA system)</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>The IP address of the internal SIP registrar server to which the RealPresence Access Director system forwards SIP registration requests from external endpoints. (This is the signaling IP address of the RealPresence DMA system)</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>The protocol the system uses for SIP signaling.</td>
</tr>
</tbody>
</table>
● Task 1: Configure Access Proxy Settings
● Task 2: Configure Basic Access Control List Settings
● Task 3: Configure System Certificates
● Task 4: Configure TURN Services
● Task 5: Provision the RealPresence Access Director System

See the Polycom RealPresence Access Director System Administrator Guide for detailed information about each of these tasks. The following sections provide specific information as it relates to this solution.

**Task 1: 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 Task 2: 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® Content Sharing Suite), and web-based video conferencing services (RealPresence CloudAXIS 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, you can create an HTTP tunnel proxy in the RealPresence Access Director system. An HTTP tunnel proxy enables RealPresence CloudAXIS Suite SIP guest users to attend video conferences in an enterprise’s CloudAXIS Suite Experience Portal. Due to restrictive firewall rules, if a CloudAXIS Suite client cannot establish a native SIP/RTP connection to a 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 guest 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.

To configure access proxy settings

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring access proxy settings. Then in the RealPresence Access Director system user interface, go to Configuration > Access Proxy Settings.

2. Configure the access proxy settings as needed for your deployment.

**Task 2: Configure Basic Access Control List Settings**

When you install a new RealPresence Access Director system, the following basic Access Control List (ACL) settings are enabled by default:

- Enable registration policy
- Allow registration from provisioned devices
To configure basic Access Control List settings

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring basic Access Control List settings. Then in the RealPresence Access Director system user interface, go to Configuration > Basic ACL Settings.

2. Configure the Registration Policy and Call Policy settings to allow access to your network. You must specifically configure which registration and call requests to allow; otherwise, the RealPresence Access Director system will deny requests.

3. Click Update.

If you need to configure advanced rules and settings to limit access to your network, see the Define Advanced Access Control List Rules topic in the Polycom RealPresence Access Director System Administrator Guide for specific instructions.

Task 3: Configure System Certificates

The RealPresence Access Director system is delivered with a self-signed certificate at installation. You can replace the self-signed certificate with a signed certificate issued by a certificate authority.

When you complete the certificate signing request, be sure to specify the following details:

- Enhanced Key Usage of the certificate must indicate both Server Authentication and Client Authentication. The RealPresence Access Director system may act as either a server or client, therefore both Server Authentication and Client Authentication are mandatory to enable a mutual TLS connection between two session border controllers.

- Key Usage must include Digital Signature and Key Encipherment.

You should configure certificates before configuring automatic provisioning of the RealPresence Access Director system and before federating or neighboring your RealPresence Access Director system with another enterprise. For more information about certificates and creating certificate signing requests, see the Polycom RealPresence Access Director System Administrator Guide.

Task 4: Configure TURN Services

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. Configuring your RealPresence Access Director system to provide STUN and TURN services is optional.

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.

For instructions on configuring TURN settings, see TURN Services in the Polycom RealPresence Access Director System Administrator Guide.

**Task 5: Provision the RealPresence Access Director System**

Configuring your RealPresence Access Director system to be provisioned by a RealPresence Resource Manager system is optional. If you choose to have your system provisioned, you must connect to the RealPresence Resource Manager system from the RealPresence Access Director user interface. Once connected, your system will be automatically provisioned with the information you configured in the RealPresence Resource Manager system.

*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.

Specifically, automatic provisioning configures the following settings:

- An NTP server for system time (Appliance Edition)
- SIP and H.323 signaling settings

*Caution: Disconnect before manually changing provisioned settings*

After you connect to a Polycom RealPresence Resource Manager system for provisioning, you cannot update the provisioned information manually in the RealPresence Access Director system until you disconnect.

**To connect to the RealPresence Resource Manager system for automatic provisioning:**

1. From the RealPresence Access Director user interface, go to **Admin > Polycom Management System**.
2. Enter the **Login Name**, **Password**, and RealPresence Resource Manager IP address for the RealPresence Access Director system user account for provisioning, and click **Connect**.

When connected, the RealPresence Resource Manager system automatically provisions the RealPresence Access Director system.

**Configure the Polycom RealPresence DMA System**

**Task 1: Enable SIP Device Authentication**

Device authentication enhances security by requiring devices registering with or calling through the RealPresence DMA system to provide credentials that the system can authenticate. In turn, the RealPresence DMA system may need to authenticate itself to an external SIP peer or neighbored gatekeeper.
All authentication configurations are supercluster-wide, but note that the default realm for SIP device authentication is the cluster’s FQDN, enabling each cluster in a supercluster to have its own realm for challenges.

**Caution: If Device Authentication is enabled, disable some RealPresence Resource Manager settings**

If Device Authentication is enabled on the RealPresence DMA system, you must disable Use Endpoint Provisioning Credentials on the RealPresence Resource Manager system.

To enable SIP authentication for ALL internal and external endpoints:

1. See the *Polycom RealPresence DMA System Operations Guide* for detailed information about enabling SIP device authentication. Then go to Admin > Local Cluster > Signaling Settings and in the SIP Settings section, select Enable authentication.
2. To add a device’s authentication credentials to the list of device credential entries that the Call Server checks, click Add and enter the user Name, Password, and Confirm Password credentials.
   - These are the credentials you set up in the RealPresence Resource Manager system to enable endpoint provisioning. They provide authentication of the endpoint’s provisioning request.

To disable SIP authentication for a specific endpoint:

1. Go to Network > Endpoints.
2. Select the endpoint for which to disable authentication.
3. Click Edit.

**Task 2: Configure an External SIP Peer to Support SIP Open B2B Calls**

To enable calls between enterprise users and external SIP endpoints that are not registered or are not members of a federated enterprise or division, you must add the RealPresence Access Director system as an external SIP peer on the RealPresence DMA system and then specify the default SIP contact ports on the RealPresence Access Director system for each transport protocol. When the RealPresence Access Director system receives a SIP request on the default contact port from a SIP endpoint that is not registered or is not a member of a federated enterprise or division, the system routes the call to the appropriate destination.

**Caution: Enabling SIP device authentication may cause some calls to fail**

If your RealPresence DMA system is peered with other SIP devices, enabling SIP device authentication may cause inbound calls to the RealPresence DMA system from those SIP peers to fail. Multiple solutions exist for resolving these issues with dial plan and network design. If necessary, please contact your Polycom field representative.
To configure an external SIP peer on the RealPresence DMA system:


2. In the External SIP Peers settings, enter the internal signaling IP address of the RealPresence Access Director system as the Next hop address.

3. In the Postliminary settings under Request URI options, select the format Use original request URI (RR).

4. Go to Admin > Call Server > Dial Rules > Add and in the Action field, select Resolve to external SIP peer. This enables the RealPresence DMA system to send an INVITE message outbound to the RealPresence Access Director system.

To configure the default local SIP contact port on the RealPresence Access Director system:

The RealPresence Access Director system routes SIP open B2B calls only if you specify a valid default contact port for each type of transport.

1. See the Polycom RealPresence Access Director System Administrator Guide for details about configuring the default contact port, then go to Configuration > SIP Settings.

2. Enter the default contact port the RealPresence Access Director system uses to receive SIP traffic from endpoints that are not registered or are not members of a federated or neighbored enterprise or division. For each type of transport (TCP, UDP, TLS), you can specify any external port not in use as the default contact port. If you are deploying a RealPresence Access Director system for the first time, the default contact ports have been pre-configured as follows:
   - TCP/UDP: 5060
   - TLS: 5061

Only one default contact port can be specified for each type of transport.

Task 3: Configure SIP Settings for Guest Users

To support SIP guest calls, you must configure the RealPresence DMA system with a dial rule prefix that corresponds to the prefix used for guests on the RealPresence Access Director system. Additionally, you must configure an external SIP port on the RealPresence Access Director system for remote (registered) users.

Polycom recommends the configurations described in the following sections:

- SIP Settings for Guest Users on the Polycom DMA System
- SIP Settings for Guest Users on the RealPresence Access Director System
- SIP Settings for Remote Users on the RealPresence Access Director System
SIP Settings for Guest Users on the Polycom DMA System

Configure these RealPresence DMA settings to correspond with guest call settings on the RealPresence Access Director system.

To configure the RealPresence DMA system to support SIP guest calls:

1. See the Configure Signaling section of the Polycom RealPresence DMA System Operations Guide for detailed information about this process. Then on the RealPresence DMA system, go to Admin > Local Cluster > Signaling Settings.
2. Add a guest dial rule prefix (SIP Settings > Unauthorized prefixes> Add) and enable Strip prefix.
3. Configure the required information so that it matches the prefix for guest calls added in the RealPresence Access Director system.
4. Go to Admin > Call Server > Dial Rules and add dial rules to handle the incoming unauthorized guest calls, one for each type of call resolution.
5. Go to Admin > Call Server > Domains and add a domain to the domain list for the host specified for guest port configuration.

SIP Settings for Guest Users on the RealPresence Access Director System

Configure these settings to enable the RealPresence Access Director system to forward SIP guest calls to the RealPresence DMA system.

To configure the RealPresence Access Director system external SIP port 5060 for guests:

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring SIP settings. Then on the RealPresence Access Director system, go to Configuration > SIP Settings.
2. Enable SIP signaling and then configure external port 5060 for SIP guest users (External Port Settings > Edit) with the required information. In this case:
   - Port name: Defaults to Unencrypted port.
   - Transport: UDP/TCP.
   - Enable Dial string policy and enter a dial string prefix (Prefix of Userinfo) that does not interfere with your dial plan and will be stripped by the RealPresence DMA system.
   - In Host, enter the host IP address or FQDN to use in the dial string. If a SIP guest user calls a domain name that differs from the Host, the RealPresence Access Director system changes the domain name and adds the Prefix of Userinfo to the dial string. For example, if a SIP guest user calls 8222@polycom.com, but the host is configured as example.com and the prefix is 77, the system will change the user's dial string to 778222@example.com.

To configure the RealPresence Access Director system external SIP port 5061 for guests:

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring SIP settings. Then on the RealPresence Access Director system, go to Configuration > SIP Settings.
2. Enable SIP signaling and then configure external port 5061 for SIP guest users (External Port Settings > Edit) with the required information. In this case:
   - Port name: Defaults to Encrypted port.
   - Transport: TLS.
- Enable **Dial string policy** and enter a dial string prefix (**Prefix of Userinfo**) that does not interfere with your dial plan and will be stripped by the RealPresence DMA system.
- In **Host**, enter the host IP address or FQDN to use in the dial string. If a SIP guest user calls a domain name that differs from the **Host**, the RealPresence Access Director system changes the domain name and adds the **Prefix of Userinfo** to the dial string. For example, if a SIP guest user calls 8222@polycom.com, but the host is configured as example.com and the prefix is 77, the system will change the user’s dial string to 778222@example.com.

**Task 4: Configure SIP Settings for Remote Users**

Configure these settings to enable remote users to register with the RealPresence DMA system.

**SIP Settings for Remote Users on the RealPresence Access Director System**

If you configure the external SIP ports 5060 and 5061 for guest users, you must add a non-standard external SIP port in the RealPresence Access Director system for remote users.

To configure a RealPresence Access Director system non-standard external SIP port to support remote user calls:

1. On the RealPresence Access Director system, go to **Configuration > SIP Settings**.
2. Enable **SIP signaling** and then configure a port for SIP registered users (**External Port Settings > Add**) with the required information. In this case:
   - **Port number**: Any non-standard port number that is not already in use.
   - **Port name**: **RegisteredUser** (for example).
   - **Transport**: Polycom suggests using TCP but UDP, UDP/TCP, or TLS may also be used. The transport protocol entered here must match the transport protocol for the RealPresence Access Director system site in the RealPresence Resource Manager system.

**Configure Polycom Endpoint Systems**

This solution supports the Polycom endpoint systems identified in **Products Supported in this Solution**.

**Task 1: Configure Polycom HDX Series Endpoints**

Polycom HDX series endpoints do not require any special set up for this solution. Polycom recommends automatic provisioning because it enables easy setup and access to advanced features.

See the Polycom HDX system documentation available at support.polycom.com for more information about configuring the endpoints for automatic provisioning.

**Task 2: Configure the Polycom Group Series System**

See the RealPresence Group Series 300 or 500 user documentation at support.polycom.com for configuration information.
Task 3: Configure Polycom RealPresence Mobile or Desktop Endpoints

For specific information on configuring RealPresence Mobile or Desktop software in this solution, refer to the online help and the Release Notes for the RealPresence Mobile or RealPresence Desktop software version you are using, available at support.polycom.com.

Professional Mode Sign-In Settings

You can choose to use your RealPresence Mobile or Desktop system in Professional Mode. In this mode, your system is automatically provisioned/configured by the RealPresence Resource Manager system. Polycom recommends automatic provisioning because it enables easy setup and access to advanced features.

The product online help describes how to configure your system for professional mode. When setting up professional mode, you must enter the user name and password configured in the RealPresence Resource Manager system to enable endpoint provisioning.

Configure the Polycom RealPresence Collaboration Server

To ensure that a RealPresence Mobile client can send content to a conference, on the RealPresence Collaboration Server, go to Setup > System Configuration > System Flags and set the value of the `NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT` system flag to at least 3.

For information about adding system flags, see "Manually Adding and Deleting System Flags" in the Polycom RMX System Administrator Guide.

After the change, you must restart the RMX system.

Integrate Two or More Systems with an 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. Integration with an F5 load balancer is optional.

The F5 load balancer acts upon data in the transport layer and serves as a TCP or UDP reverse proxy to distribute (balance) incoming sign-in, registration, and call requests across multiple RealPresence Access Director systems. 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.

The F5 load balancer must be configured to integrate with your RealPresence Access Director systems, but no configuration is necessary on the RealPresence Access Director systems.
F5 Load Balancer Configuration Requirements

To ensure that an F5 load balancer operates correctly with your RealPresence Access Director systems, the F5 system configuration must meet the following requirements:

- The F5 system terminates traffic flow on the transport layer and works as a UDP or TCP reverse proxy. A port-based virtual server should be defined on the load balancer to support the following port assignments:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 RAS</td>
<td>1719</td>
</tr>
<tr>
<td>H.323 Call Signaling</td>
<td>1720</td>
</tr>
<tr>
<td>SIP</td>
<td>5060, 5061, other SIP ports</td>
</tr>
<tr>
<td>HTTPS Proxy</td>
<td>443</td>
</tr>
<tr>
<td>LDAP Proxy</td>
<td>389</td>
</tr>
<tr>
<td>XMPP Proxy</td>
<td>5222</td>
</tr>
</tbody>
</table>

- The F5 system uses the Round Robin algorithm for load balancing and failovers.
- The F5 system routes only incoming sign-in, registration, and call requests. The load balancer does not affect the outgoing calls from the enterprise network to the Internet.
- The F5 load balancer must have a heartbeat connection between all RealPresence Access Director systems to ensure that requests are routed only to an accessible system. During a failover, the load balancer routes requests to a different RealPresence Access Director system, based on the RealPresence Access Director system priority group.
- The routing policy of the F5 load balancer must support persistence. Persistence ensures that all requests from the same source IP address during a session are distributed to the same RealPresence Access Director system.
- At a minimum, the F5 load balancer should support the following scenarios:
  - Remote endpoint (EP) login to the RealPresence Resource Manager system
  - Remote SIP EP registration to the RealPresence DMA system (TLS/TCP)
  - Remote SIP EP incoming call
  - Remote H.323 EP registration to the RealPresence DMA system (H.460/ non-H.460)
  - Remote H.323 EP incoming call
  - Guest SIP EP incoming call
  - Guest H.323 EP incoming call
  - Trusted H.323 B2B incoming call
  - RealPresence CloudAXIS suite incoming HTTP tunnel call

F5 Load Balancer Impacts on other RealPresence Access Director System Features

Some RealPresence Access Director system functions may not operate correctly when the systems are deployed with an F5 load balancer. The following features are affected:
● When HTTPS, LDAP, and XMPP requests pass through the F5 system, the RealPresence Access Director system does not know the source IP address of the remote device. As a result, the following settings do not function:

  ➢ **Enable access proxy white list authentication for LDAP and XMPP access.** See Admin > Security Settings in the RealPresence Access Director system web user interface.

  ➢ **Allow registration from provisioned devices.** See Configuration > Basic ACL Settings in the web user interface. *Note that other basic ACL settings may not function correctly.*

● The RealPresence Access Director system treats a trusted B2B call as a guest call because the source IP address is unknown.

  ➢ To configure the RealPresence Access Director system to allow a trusted H323 B2B call, you must enable the **Allow any incoming LRQ** option. See Configuration > H.323 Settings.
Deploying Two RealPresence Access Director Systems in a Tunnel Configuration

Two RealPresence Access Director systems can be deployed in a tunnel configuration. In this model, one system is deployed as the tunnel server in the corporate back-to-back 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, while 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 Task 3: Activate the System Licenses for Appliance Edition Servers.

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, media, and access proxy 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

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.

See these topics for detailed information about tunnel configuration settings:

- Configure the DNS Service for the Two-System Tunnel
- Configure Firewalls and Ports
- Install and Configure the RealPresence Access Director Systems
- Configure the RealPresence Resource Manager System
- Configure the Polycom RealPresence DMA System
- Configure Additional Polycom Components

Configure the DNS Service for the Two-System Tunnel

For complete DNS service configuration instructions, see Chapter 6, “Deploying the RealPresence Access Director System in a Corporate DMZ Environment,” Configure the DNS Service in this guide.

For a tunnel deployment, the IP address to use when you create the RealPresence Access Director system DNS A record for the internal DNS server depends on whether the tunnel client has one or two network interfaces. Use the following information to determine the correct IP address for the DNS A record:

- One network interface: The IP address of the tunnel client. This IP address matches the Local tunnel client address field in the tunnel client settings.
- Two network interfaces: The internal signal and media IP address of the tunnel client. This IP address matches the Internal signaling/media/access proxy IP of tunnel client field in the tunnel client settings.

The example below assumes your tunnel client has two network interfaces.

- If the FQDN of the RealPresence Access Director system is rpad.example.com, and the internal signaling and media IP address of the tunnel client is 10.22.210.111, create an A record as shown below:
  rpad.example.com IN A 10.22.210.111

Configure Firewalls and Ports

Follow these guidelines for configuring your firewalls.

Caution

If you’re not familiar with firewall concepts and administration and your enterprise’s firewall implementation, please consult with someone who is. For greater security, Polycom recommends that you disable SSH and web access connectivity from the Internet, and enable SSH and web access connectivity from the LAN.
Outside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Configure 1:1 NAT
- Set interface mode to NAT
- Disable H.323 and SIP ALG
- Disable any H.323 helper services on the firewall (for example, Cisco® H.323 Fixup).

Inside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Disable H.323 and SIP ALG
- Disable any H.323 helper services on the firewall (for example, Cisco® H.323 Fixup).

Caution: Disable predefined services in your firewall

When you deploy the RealPresence Access Director system, you must disable all predefined services, such as SIP ALG and H.323 ALG, in your firewall. After these services are disabled, create port and protocol rules for the functionality you need in your implementation. See Required Ports.

Install and Configure the RealPresence Access Director Systems

Task 1: Perform Basic Installation


Task 2: Synchronize the Time and Set the Time Zones

After initial installation of the RealPresence Access Director systems, configure the time settings as follows:

- Synchronize the time on the tunnel server and tunnel client to the same Network Time Protocol (NTP) server before encrypting the tunnel between the two systems (if applicable).
- Select the time zone of your geographic location on the two systems.

To configure the time settings:

1. From a browser, go to the IP address of the tunnel server.
2. Go to Admin > Time Settings.
3. In System time zone, select the time zone of your specific geographic location.
4 In NTP servers, enter the IP address or FQDN of the NTP server with which to synchronize. Polycom recommends that you configure at least two NTP servers. If you deploy two RealPresence Access Director, Virtual Edition systems, you can configure up to three NTP servers from the RealPresence Platform Director system.

5 Click Update and OK to accept your settings and restart the system.

6 Repeat the above steps from the user interface of the tunnel client.

Task 3: Activate the System Licenses for Appliance Edition Servers

If you deploy two RealPresence Access Director Appliance Edition systems in a tunnel configuration, you must activate the license for each system. The license with the fewest number of calls reflects the total number of licensed calls that can traverse the two-system tunnel.

After activating both licenses, you can view the number of licensed calls from the Dashboard of both the tunnel server and the tunnel client.

To activate the tunnel server license:

1. From a browser, go to the IP address of the tunnel server.
2. Log into the RealPresence Access Director system user interface and go to Maintenance > License.
3. Enter the Activation key for the tunnel server license and click Update.
   The system restarts.

To activate the tunnel client license:

1. From a browser, go to the IP address of the tunnel client.
2. Log into the RealPresence Access Director system user interface and go to Maintenance > License.
3. Enter the Activation key for the tunnel client license and click Update.
   The system restarts.

Task 4: Configure Network Settings for the Tunnel Server

Network settings for the tunnel server can be configured for one to four network interfaces.

To configure network settings for the tunnel server:

1. See the Polycom RealPresence RealPresence Access Director System Administrator Guide for detailed information about configuring network settings for the tunnel server. Then 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 and click Next.
4. In the Step 2 of 3: Advanced Network Settings window, click each of the network interfaces to configure and enter the following information.
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.

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 and to the tunnel itself 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 management through the web-based 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 (see Task 6: 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.

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

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

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

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

**Task 5: Configure Network Settings for the Tunnel Client**

Network settings for the tunnel client can be configured for one to three network interfaces.

To configure network settings for the tunnel client:

1 See the Polycom RealPresence RealPresence Access Director System Administrator Guide for detailed information about configuring network settings for the tunnel client. Then 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 and click Next.

4 In the Step 2 of 3: Advanced Network Settings window, click each of the network interfaces to configure and enter the following information.
5 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 **Tunnel Client Network Interface Configuration**.

6 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, media, and access proxy communication with the RealPresence DMA system. See the **Internal signaling/media/access proxy IP of tunnel client** field in **Task 7: Configure Two-Box Tunnel Settings on the Tunnel Client**.

### Task 6: Configure Two-Box Tunnel Settings on the Tunnel Server

If your license supports tunnel encryption, you must first synchronize the time on the tunnel server and the tunnel client to the same Network Time Protocol (NTP) server before encryption. See **Task 2: Synchronize the Time and Set the Time Zones**.

**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>
<tr>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Select <strong>Server</strong> to enable the system to operate as a tunnel server.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
</tr>
<tr>
<td>Encrypted tunnel</td>
<td>When selected, communications between the tunnel server and tunnel client are encrypted.</td>
</tr>
</tbody>
</table>

**Note:** 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.

*This setting must be the same on both the tunnel server and tunnel client.*
Task 7: Configure Two-Box Tunnel Settings on the Tunnel Client

If your license supports tunnel encryption, ensure that the time settings on the tunnel server and the tunnel client have been synchronized to the same NTP server before encrypting the tunnel. See Task 2: Synchronize the Time and Set the Time Zones.

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 below 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>
<tr>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Select Client to enable the system to operate as the tunnel client.</td>
</tr>
</tbody>
</table>
| Encrypted tunnel    | When selected, communications between the tunnel server and tunnel client are encrypted.  
                       | **Note:** This option displays only if you purchase a license that supports encryption of the tunnel between two systems. Select this option to encrypt the tunnel communications.  
                       | This setting must be the same on both the tunnel server and tunnel client. |
The system restarts and the two-system tunnel connection status displays on the user interface Dashboard on both the tunnel server and tunnel client.

**Task 8: Configure System Certificates**

The tunnel connection between the tunnel server and client uses a default self-signed certificate dedicated for tunnel use. This certificate cannot be changed but can be refreshed when it expires.

In addition to the tunnel certificate, you must add a certificate authority’s public certificate and create a certificate signing request to obtain a signed certificate for the RealPresence Access Director system. For instructions, see the *Polycom RealPresence Access Director System Administrator Guide*.

You should configure certificates before federating your RealPresence Access Director system with other enterprises.

**Task 9: Configure Access Control List Rules and Rule Settings**

See *Task 2: Configure Basic Access Control List Settings* in *Deploying the RealPresence Access Director System in a Corporate DMZ Environment*.

**Configure the RealPresence Resource Manager System**

In a two-box tunnel configuration, the RealPresence Resource Manager system does not provision the tunnel server or tunnel client but does provision endpoints through the RealPresence Access Director system.

---

**Field** | **Description**
---|---
Performance profile | If you enable tunnel encryption, select a performance profile. **Premium**: 10 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 600M **Regular**: 6 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 400M **Base**: 2 CPU core are allocated to tunnel processes. Maximum tunnel throughput: 200M *The profiles on the tunnel server and client must match.*

* Local tunnel client address | The IP address and port number of the tunnel client. Default port: 1194 **Note**: Polycom recommends that you use the default port number 1194, but you can use any value from 1190-1199 or 65380-65389.

* Remote tunnel server address | The IP address and port number of the tunnel server. Default port: 1194

* Internal signaling/media/access proxy IP of tunnel client | The IP address of the network interface that the tunnel client uses for internal signaling, internal media, and internal access proxy communication with the RealPresence DMA system.

3 Click **Update**. The system restarts and the two-system tunnel connection status displays on the user interface Dashboard on both the tunnel server and tunnel client.
To enable endpoint provisioning, configure the following information in the RealPresence Resource Manager system. For detailed instructions, see The Polycom® RealPresence® Resource Manager System Operations Guide.

- Create a site for the RealPresence Access Director system
- Create an RPAD server provisioning profile
- Create a network provisioning profile for endpoints
- Create a provisioning rule and associate it with all related profiles
- Create a user account for the RealPresence Access Director system

**Configure the Polycom RealPresence DMA System**

See Configure the Polycom RealPresence DMA System in Deploying the RealPresence Access Director System in a Corporate DMZ Environment.

**Configure Additional Polycom Components**

Refer to the following sections in Deploying the RealPresence Access Director System in a Corporate DMZ Environment to configure additional Polycom components.

- Configure Polycom Endpoint Systems
- Configure the Polycom RealPresence Collaboration Server
Deploying RealPresence Access Director Systems with High Availability

Two Polycom® 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, which helps to ensure that users always have access to a RealPresence Access Director system within your network.

This section provides information specific to a High Availability environment. For complete deployment details, see Deploying the RealPresence Access Director System in a Corporate DMZ Environment.

The following topics provide details about High Availability:

- High Availability Overview
- Network Settings to Support High Availability
- Configure Network Settings
- High Availability Requirements
- Configure High Availability Settings
- Firewall Configuration
- High Availability Status
- Log Files
- Licensing
- Certificates
- DNS Records

High Availability Overview

High Availability enables two RealPresence Access Director systems on the same network to operate within an active-active architecture. This means that both systems run concurrently and are able to proxy calls and registrations.

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 users 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.

**Failovers**

After High Availability is enabled and configured, the two systems communicate status by sending a heartbeat signal to the network interfaces configured as HA links. If one system does not receive a heartbeat signal from at least one HA link on the other system within a certain time period, a dynamic failover occurs. During a failover, the system that is operating correctly takes over the resources (virtual IP addresses and the associated services) of the system that failed.

The following situations will cause a failover to occur:

- A server fails
- All HA links fail (if at least one HA link is running normally, a failover will not occur.)
- A network interface with a virtual IP address fails (if more than one NIC has a virtual IP address, all resources will be taken over, not just those associated with the failed NIC)

If a direct link fails (e.g., the cable is disconnected), the network interfaces with virtual IP addresses may remain active. In this situation, a failover does not occur. Both systems will report the failure of the direct HA link but neither system will take over the resources of the other. When you reconnect or repair the direct link, the two systems will automatically reconnect.

A system failover typically requires approximately 10 seconds for all resources to be available on the peer system. Note that the failover times may be longer depending on what caused the failover.

When a system that failed is running again, it requests its original resources back from the peer system. If the peer system does not have any active calls, it releases the resources back to the system that previously failed. If the peer system has active calls, it will release the resources approximately 2 minutes after its final active call ends.

If you prefer to choose the time when a peer system releases resources back to the other system, you can manually force the release of resources at the time you choose. To do so, log in to the user interface of the peer system and go to Diagnostics > High Availability Status > Release Peer Resources.

**Network Settings to Support High Availability**

When you configure the network settings for your two RealPresence Access Director systems, consider the following information about High Availability that may affect how you configure your settings:

- Configure the network settings for all network interface cards (NICs) on each system before you enable High Availability and configure its settings. Once HA is enabled, configuring network settings is disabled.
- The physical IP addresses of the same network interfaces on each system (e.g., eth1 and eth1) must be on the same subnet.
- Assign the same services to the same network interfaces on each system.
- Network interfaces assigned to media traffic should not be used as HA links.
- If you plan to configure one or more network interfaces as dedicated HA links (no assigned services), you need to assign IP addresses based on the physical location of your two RealPresence Access Director systems:
- If the two systems are located physically close to each other and the direct link cable does not need to be routed within your network, the IP addresses you assign to the dedicated HA interfaces do not need to be within your network IP space but they must be on the same subnet.
- If your two systems are not located in the same area, the IP addresses you assign to the dedicated HA interfaces must be within your network IP space and on the same subnet.

### Network Interface Configuration Options

The settings you configure for your network depend on various factors, including your network architecture and policies. The following table provides two possible options for configuring the network interfaces on each of your RealPresence Access Director systems to support High Availability. These options may or may not be suitable within your own network environment.

<table>
<thead>
<tr>
<th>Number of NICs</th>
<th>Name of Interface</th>
<th>Assigned Services Option 1</th>
<th>Assigned Services Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy&lt;br&gt;Internal SIP/H.323 signaling and access proxy&lt;br&gt;External media&lt;br&gt;Internal media&lt;br&gt;Management&lt;br&gt;TURN&lt;br&gt;High Availability</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>Management&lt;br&gt;High Availability</td>
<td>Management&lt;br&gt;High Availability&lt;br&gt;External SIP/H.323 signaling and access proxy&lt;br&gt;Internal SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External SIP/H.323 signaling and access proxy&lt;br&gt;Internal SIP/H.323 signaling and access proxy&lt;br&gt;External media&lt;br&gt;Internal media&lt;br&gt;TURN</td>
<td>External media&lt;br&gt;Internal media</td>
</tr>
</tbody>
</table>
Configure Network Settings

After you determine the settings that are appropriate for your network, log in to the web user interface of each RealPresence Access Director system and configure the network settings.

**Configure network interfaces consecutively**

When you configure network interfaces, you must assign an IP address, subnet mask, and default gateway to consecutive NICs. For example, if you configure three NICs, you must configure eth0, then eth1, then eth2.

See the Polycom RealPresence Access Director System Administrator Guide for additional details about configuring network settings.

**To configure network settings:**

1. Go to Admin > Network Settings > Configure Network Settings.
2 In the **Step 1 of 3: General Network Settings** window, confirm or reconfigure the general network settings for the system.

3 Click **Next**.

4 In the **Step 2 of 3: Advanced Network Settings** window, click each of the network interfaces *consecutively* to configure and complete the following fields.
   - **IPv4 Address**: Remember that the physical IP addresses assigned to the *same network interfaces on each server* (for example, eth1) *must be on the same subnet*.
   - **IPv4 Subnet Mask**
   - **IPv4 Default Gateway**

5 Click **Next**.

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

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

## High Availability Requirements

Consider the following requirements before you configure your High Availability settings:

- Ensure that all other settings for the RealPresence Access Director system are configured identically on both systems. For standard deployment details, see *Deploying the RealPresence Access Director System in a Corporate DMZ Environment* in this guide. For instructions on configuring all system settings, see the *Polycom RealPresence Access Director System Administrator Guide*.

- Configure a virtual IP address for at least one network interface. Assign a different virtual IP address for the corresponding network interface on the peer system. If you configure more than one network interface, assign virtual IP addresses to the interfaces used for signaling traffic.

- A virtual IP address must be on the same subnet as the physical IP address for the NIC.

- Configure at least one network interface as an HA link. The HA link can be a connection to the physical IP address of the same NIC on the peer system or it can be a direct link. A direct link physically connects two network interfaces on a private network. Use one or both of the following settings to configure an HA link:
  - **Enable Interface for HA traffic**: When enabled, the network interface can act as a dedicated HA link or it can also have assigned services. If you select this option, you must provide the physical IP address of the same NIC on the peer system.
  - **Use Direct Link**: When enabled, the network interface acts as a dedicated HA link and cannot have assigned services.

- If a network interface is dedicated only to HA traffic (that is, it has no services assigned), it does not require a virtual IP address.

- HA cannot be configured if a two-system tunnel is enabled. Likewise, if HA is enabled, the two-system tunnel is disabled.

- When HA is enabled, **Configure network settings** is disabled.

- The two systems configured for High Availability use ports 65011 and 65012 for TCP and UDP communication between them. Internal traffic must be routable if the systems do not have a direct link. *Note that these two ports do not need to be open on the firewall.*
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.

Enter required information for all NICs before you submit your HA settings

When you configure High Availability settings, you need to enter the required information for each active NIC before you submit your settings. If you try to submit partial settings, you may have errors that result from missing information.

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 Local Physical IP Address, Local Virtual IP Address, and Peer Virtual IP Address 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. 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>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>
</tbody>
</table>
After you configure each network interface, click **Submit**.

The system reboots.

After the system restarts, go to **Admin > High Availability Settings**.

Click **Configure Peer** to apply the same settings to the peer system.

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 system reboots.
6. After the system restarts, go to Admin > High Availability Settings.
7. Click Configure Peer.
8. Enter the name and password and click OK.
   A message displays that the peer system was successfully configured and the peer system reboots.
   After it restarts, all HA settings are applied to the peer system, including the new password.

Firewall Configuration

For overall information on configuring your firewalls, see Configure Firewalls and Ports.

For the High Availability solution, you must map public IP addresses on your firewall to specific virtual or physical IP addresses on both RealPresence Access Director systems. Polycom recommends two different options for configuring your firewall.

Configuration of the RealPresence Resource Manager system
If you use a RealPresence Resource Manager system to dynamically provision endpoints, you need to create a separate site for each RealPresence Access Director system public IP address that maps to a virtual IP address. See Configure the RealPresence Resource Manager System.
Option 1: Two Public IP Addresses (NAT Required)

The following table describes a firewall configuration with two NATed public IP addresses:

<table>
<thead>
<tr>
<th>Public IP Address on Firewall</th>
<th>Name of RealPresence Access Director System</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP Address 1</td>
<td>System 1</td>
<td>Virtual IP address of the network interface for external signaling and access proxy</td>
<td>Ports used for external signaling and external access proxy (see SIP WAN Ports, H.323 WAN Ports, Access Proxy WAN Ports)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical IP address of the network interface for external media</td>
<td>Ports used for external media (see Media WAN Ports)</td>
</tr>
<tr>
<td>Public IP Address 2</td>
<td>System 2</td>
<td>Virtual IP address of the network interface for external signaling and access proxy</td>
<td>Ports used for external signaling and external access proxy (see SIP WAN Ports, H.323 WAN Ports, Access Proxy WAN Ports)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical IP address of the network interface for external media</td>
<td>Ports used for external media (see Media WAN Ports)</td>
</tr>
</tbody>
</table>

Option 2: Four Public IP Addresses (NAT not Required)

The following table describes a firewall configuration with four public IP addresses:

<table>
<thead>
<tr>
<th>Public IP Address on Firewall</th>
<th>Name of RealPresence Access Director System</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP Address 1</td>
<td>System 1</td>
<td>Virtual IP address of the network interface for external signaling and access proxy</td>
<td>Ports used for external signaling and external access proxy (see SIP WAN Ports, H.323 WAN Ports, Access Proxy WAN Ports)</td>
</tr>
<tr>
<td>Public IP Address 2</td>
<td>System 1</td>
<td>Physical IP address of the network interface for external media</td>
<td>Ports used for external media (see Media WAN Ports)</td>
</tr>
</tbody>
</table>
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 needed to update the information.

Log Files

Any changes in state of the RealPresence Access Director system or High Availability will force an event to the system. These events are then logged appropriately.

Events related to system services are recorded in the server.log file. High Availability events, such as HA configuration changes and failover events are recorded in the ha_availability.log file.

View Log Files

To view a log file, you must first download it and save it locally.

To view 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.
3. Select a log file to download.
4. Under Actions, select Download Logs.
5. In the Save As dialog, select a location, and choose Save.
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>
<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>

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.
Certificates

When you deploy two RealPresence Access Director systems for High Availability, each system has a default self-signed SSL certificate. To ensure that both of your systems are identified as trusted entities, Polycom highly recommends that you request a signed identity certificate from a Certificate Authority (CA). Additionally, you need to install your chosen CA’s public certificate in the TRUSTED_STORE on each system before you enable and configure High Availability settings.

Read Managing Certificates in the Polycom RealPresence Access Director System Administrator Guide

Before you request or install certificates, Polycom highly recommends that you review complete information about managing certificates in the Polycom RealPresence Access Director System Administrator Guide.

After you configure the network and High Availability settings, submit a Certificate Signing Request (CSR) to obtain a signed certificate for each system. Each CSR must include the FQDN and domain of the individual RealPresence Access Director system and Subject Alternative Names (SANs) for the following:

- Virtual hostnames* for interfaces on the individual RealPresence Access Director system
- Virtual IP addresses for interfaces on the individual RealPresence Access Director system
- Virtual hostnames for interfaces on the peer RealPresence Access Director system
- Virtual IP addresses for interfaces on the peer RealPresence Access Director system

* See Configure High Availability Settings for the characters allowed in hostnames.

After you receive the signed certificates, install both certificates in the KEY_STORE of both RealPresence Access Director systems.

DNS Records

Your RealPresence Access Director systems must be accessible by their host name(s), not just their IP address(es), so you (or your DNS administrator) must create the necessary A records, as well as the corresponding PTR records, on your DNS server(s).

A records and PTR records that map each physical host name to the corresponding physical IP address and each virtual host name to the corresponding virtual IP address are mandatory, as are the corresponding PTR records that allow reverse DNS resolution of the system’s physical or virtual host name(s).

For further details about DNS records required for the RealPresence Access Director system, see Configure the DNS Service in Deploying the RealPresence Access Director System in a Corporate DMZ Environment.

Fully Qualified Domain Names

Depending on local DNS configuration, a host name could be the RealPresence Access Director system’s fully qualified domain name (FQDN) or a shorter name that DNS can resolve.
Federation Between RealPresence Access Director Systems

This chapter describes how to configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises. In the deployment solution described in this chapter, each division or enterprise must have a RealPresence Access Director system.

In this chapter, we assume you have already performed the standard deployment as documented in Deploying the RealPresence Access Director System in a Corporate DMZ Environment.

Federation in a SIP Environment

To configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises in a SIP environment, each division or enterprise must have a RealPresence Access Director system that is configured:

- To trust the other’s Certificate Authority (CA) certificate
- With mutual TLS enabled
- With a default route to the other’s Real Presence Access Director system.

In addition, the federated enterprises must:

- Have a dial plan to route traffic to and from specific ports using specified protocols
- Directed to the designated port

To support SIP calls from federated divisions or enterprises, complete the following tasks:

- **Task 1:** Create Additional DNS SRV Records on the External DNS Server
- **Task 2:** Obtain and Install the Certificates for the RealPresence Access Director Systems
- **Task 3:** Configure the RealPresence Access Director Systems to Support Federated SIP Calls
- **Task 4:** Configure the Polycom RealPresence DMA Systems to Support Federated SIP Calls

**Task 1: Create Additional DNS SRV Records on the External DNS Server**

Configure the DNS Service describes the basic DNS setup required for this solution. Federating sites requires additional DNS configuration as described in this section.

**Note: Complete DNS records for the two sites being federated**

Complete this process on the DNS systems for the two sites being federated. If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.
Create an SRV record on the external DNS server you specified in Admin > Network Settings in the RealPresence Access Director system. This SRV record maps the SRV service address to the FQDN of the RealPresence Access Director system. The SRV record is required by the Auto Find Provisioning Server feature of dynamically-managed endpoints.

So if the RealPresence Access Director system has the FQDN name `rpad.example.com`, add an SRV record as follows.

```
_sips._tcp.example.com. IN SRV 0 0 5060 rpad.example.com.
```

**Task 2: Obtain and Install the Certificates for the RealPresence Access Director Systems**

Each of the RealPresence Access Director systems in a SIP federation must have a signed Certificate Authority (CA) certificate and each certificate must be installed on both RealPresence Access Director systems.

To request a certificate for your RealPresence Access Director system, create a Certificate Signing Request and submit it to your trusted CA. When you receive the signed certificate, install it in the `KEY_STORE` of your system. Then, obtain the CA certificate of the other RealPresence Access Director system and install it in your system’s `TRUSTED_STORE`.

The system administrator of the other RealPresence Access Director system must complete the same process.

See the following topics in the Polycom RealPresence Access Director System Administrator Guide for additional details:

- Create a Certificate Signing Request
- Add the Signed Certificate to the KEY_STORE
- Add a Certificate from a Trusted Connection

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

The certificate is added to the TRUSTED_STORE of your RealPresence Access Director system.

**Task 3: Configure the RealPresence Access Director Systems to Support Federated SIP Calls**

Complete the following configuration steps on each enterprise’s or division’s RealPresence Access Director system.
To configure the federated sites’ RealPresence Access Director systems to support SIP calls:

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring SIP settings. Then go to Configuration > SIP Settings.

2. **Enable SIP signaling** and add a port for SIP users (External Port Settings > Add) and configure the required information.
   - Transport protocol must be TLS (mutual TLS).
   - **Require certificate from remote endpoint** must be selected.

3. Go to Configuration > Federation Settings > Add and configure the required information for the federated sites.
   - In **Company Address** enter the FQDN or IP address of the federated site’s RealPresence Access Director system.

4. Go to Admin > Certificates and verify that the federated site’s CA certificate for the RealPresence Access Director system is in the TRUSTED_STORE.

**Task 4: Configure the Polycom RealPresence DMA Systems to Support Federated SIP Calls**

Each enterprise’s or division’s RealPresence DMA system must be configured to support SIP federated calls. Use the following steps to configure both RealPresence DMA systems.

To configure the federated sites’ RealPresence DMA systems to support federated SIP calls:

1. See the Polycom RealPresence DMA System Operations Guide for detailed information about adding an external SIP peer. Then go to Network > External SIP Peer > Add.

2. On the **External SIP Peer** tab, enter the following information:
   - **Next hop address**: the internal signaling IP address of the RealPresence Access Director system.
   - **Port**: the internal SIP port of the RealPresence Access Director system used for communication between the RealPresence Access Director system and the RealPresence DMA system.

3. On the **Postliminary** tab, set Request URI options to Use original request URI (RR).

4. On the **Authentication** tab, click Add and add the federated site’s authentication information.

5. Go to Admin > Call Server > Device Authentication and add the federated site’s authentication credentials to the list of device credential entries that your call server should check.

6. Select the **Inbound Authentication** tab, click Add and add the local system’s authentication information for inbound messages.

7. Select the **Shared Outbound Authentication** tab, click Add and add the federated site’s authentication information for outbound messages.

8. Go to Admin > Local Cluster > Signaling Settings and in the SIP Settings section, select Enable SIP signaling and Enable authentication.

9. Go to Admin > Call Server > Dial Rules and add a dial rule for federated site’s RealPresence Access Director system that resolves to external SIP peer, so the RealPresence DMA system can send the INVITE message out to the RealPresence Access Director system.
Go to Admin > Call Server > Domains and add the local RealPresence Access Director system to the domain list.

Federation in an H.323 Environment

To configure this solution to support calls between endpoint users in two separate but neighbored (trusted) divisions or enterprises in an H.323 environment, each division or enterprise must have a RealPresence Access Director system that is configured:

- With a dial plan to route E.164 aliases properly between the enterprises
- To be directed to the designated port

To support H.323 calls from neighbored divisions or enterprises, perform the following deployment tasks:

- Task 1: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls
- Task 2: Configure the Polycom RealPresence DMA Systems to Support Federated H.323 Calls

Task 1: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls

Each enterprise’s or division’s RealPresence Access Director system must be configured to support neighbored H.323 neighbored calls. Use the following steps to configure both RealPresence Access Director systems.

To configure the neighbored enterprises’ RealPresence Access Director systems to support H.323 calls:

1. See the Polycom RealPresence Access Director System Administrator Guide for detailed information about configuring H.323 settings. Then go to Configuration > H.323 Settings.

2. Enable H.323 signaling and configure the required information.
   - Gatekeeper (next hop) address is the RealPresence DMA system IP address.
   - CIDR IP addresses are based on the RealPresence DMA system configurations:
     - If the RealPresence DMA system is set to direct mode, the CIDR IP addresses must include all internal endpoints and the same side’s SBC IP addresses.
     - If two RealPresence DMA systems are configured as a cluster, the CIDR IP addresses should include all gatekeeper addresses.
     - If the RealPresence Access Director system is deployed for registration, the SBC net of the RealPresence DMA system’s site setting should have the RealPresence Access Director system’s IP address for open B2B.

3. Go to Configuration > Federation Settings > Add and configure the required information for the federated enterprise.
   - Enter the IP address of the federated site’s system.

Note: Port used during call is returned by DNS SRV search
Generally, you will not need to configure the remote RAS port and H.225 signaling ports. The port used during the call will be returned by the DNS SRV search.
Task 2: Configure the Polycom RealPresence DMA Systems to Support Federated H.323 Calls

Each enterprise’s or division’s RealPresence DMA system must be configured to support neighbored H.323 calls. Use the following steps to configure both RealPresence DMA systems.

To configure the neighbored enterprises’ RealPresence DMA systems to support H.323 calls:

1. See the Polycom RealPresence DMA System Operations Guide for detailed information about adding a neighbored gatekeeper. Then go to Network > External Gatekeeper > Add and add the local RealPresence Access Director system as a neighbored gatekeeper identified by its internal signaling address.

2. Go to Admin > Call Server > Dial Rules and add a “resolve to external gatekeeper” dial rule for the local RealPresence Access Director system that has been identified as the gatekeeper.

3. Go to Admin > Call Server > Domains and add the local RealPresence Access Director system to the domain list.
Federation Between RealPresence Access Director and Other Systems

The RealPresence Access Director system can be configured to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises. This section describes how to configure the solution when one of the federated sites has a RealPresence Access Director system and the other site has a different session border controller. Supported solutions include:

- Federation in an H.323 Environment with Polycom VBP-E Systems
- Federation in a SIP Environment with Acme Packet

In this chapter, we assume you have already performed the standard deployment for the applicable systems as documented in Deploying the RealPresence Access Director System in a Corporate DMZ Environment.

Federation in an H.323 Environment with Polycom VBP-E Systems

In this solution deployment model, two enterprises or divisions are federated. One of the federated enterprises has a RealPresence Access Director system as its access controller along with a RealPresence DMA system as gatekeeper. The other federated enterprise has a Polycom VBP 5300E as its access controller and uses either an embedded or Polycom CMA system v6.2 gatekeeper.

To support calls between these federated divisions or enterprises, perform the following deployment tasks:

- Task 1: Create an Additional DNS A Record on the External DNS Server
- Task 2: Create Additional DNS SRV Records on the External DNS Server
- Task 3: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls
- Task 4: Configure the Polycom RealPresence DMA System to Support Federated H.323 Calls
- Task 5 (Conditional): Configure the CMA System to Support Federated H.323 Calls
- Task 6 (Conditional): Configure the VBP-5300E System to Support Federated H.323 Calls
- Task 7 (Conditional): Configure the VBP-5300E System in Embedded Gatekeeper Mode to Support Federated H.323 Calls

Task 1: Create an Additional DNS A Record on the External DNS Server

Configure the DNS Service describes the basic DNS setup required for the RealPresence Access Director system in this solution. Federation requires additional DNS configuration as described here.

Note: If necessary, get help with configuring the DNS records

If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.
Create a DNS A (address) record on the external DNS server to map the FQDN of the VBP 5300E system to its public (WAN side) IP address.

So if the VBP-E system has the FQDN name `vbpe_b.example2.com`, add an A record as follows:

```
vbpe_b.example2.com  IN A 192.168.11.100
```

**Task 2: Create Additional DNS SRV Records on the External DNS Server**

Each access controller—the RealPresence Access Director system and the VBP 5300E system must have an SRV record on the external DNS server to map the SRV service address to its FQDN.

- Create an SRV record on the external DNS server to map the SRV service address to the FQDN of the RealPresence Access Director system.

  The SRV record is required by the *Auto Find Provisioning Server* feature of the RealPresence Mobile system.

  So if the RealPresence Access Director system has the FQDN name `rpad.example.com`, add SRV records as follows.

  ```
  _h323ls._udp.example.com.  IN SRV 0 0 1719 rpad.example.com.
  _h323cs._tcp.example.com.  IN SRV 0 0 1720 rpad.example.com.
  ```

- Create an SRV record on the external DNS server to map the SRV service address to the public IP address of the Polycom VBP-5300E system.

  So if the VBP-E system has the FQDN name `vbpe_b.example2.com`, add SRV records as follows.

  ```
  _h323ls._udp.example2.com.  IN SRV 0 0 1719 vbpe_b.example2.com
  _h323cs._tcp.example2.com.  IN SRV 0 0 1720 vbpe_b.example2.com
  ```

**Task 3: Configure the RealPresence Access Director Systems to Support Neighbored H.323 calls**

Each enterprise’s or division’s RealPresence Access Director system must be configured to support neighbored H.323 calls.

**Note: Classless Inter-Domain Routing (CIDR) notations**

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.

**To configure the federated enterprises’ RealPresence Access Director systems to support federated H.323 calls:**

1. **See the Polycom RealPresence Access Director System Administrator Guide** for detailed information about configuring H.323 settings. Then go to *Configuration > H.323 Settings*.

2. **Enable H.323 signaling** and configure the following gatekeeper and network settings.
   - Gatekeeper (next hop) address is the RealPresence DMA system IP address.
   - Classless Inter-Domain Routing (CIDR) should only include the subnet of the internal gatekeeper.
3 Go to Configuration > Federation Settings > Add and configure the required information for the federated enterprise.
   - Enter the FQDN or IP address of the federated site’s VBP-E system.
   - Complete the other tabs and fields of the dialog as required

Note: Port used during call is returned by DNS SRV search
Generally, you will not need to configure the remote RAS port and H.225 signaling ports. The port used during the call will be returned by the DNS SRV search.

**Task 4: Configure the Polycom RealPresence DMA System to Support Federated H.323 Calls**

Each enterprise’s or division’s RealPresence DMA system must be configured to support neighbored H.323 calls.

To configure the federated enterprise’s RealPresence DMA systems to support federated calls:

1 See the *Polycom RealPresence DMA System Operations Guide* for detailed information about adding a neighbored gatekeeper. Then go to Network > External Gatekeeper > Add and add the local RealPresence Access Director system as a neighbored gatekeeper identified by its internal signaling address.

2 Go to Admin > Call Server > Dial Rules and add a “resolve to external gatekeeper” dial rule for the local RealPresence Access Director system that has been identified as the gatekeeper.

**Task 5 (Conditional): Configure the CMA System to Support Federated H.323 Calls**

If a CMA system is the gatekeeper for the federated enterprise using the VBP-E access controller, perform this task. Otherwise, skip to Task 7 (Conditional): Configure the VBP-5300E System in Embedded Gatekeeper Mode to Support Federated H.323 Calls.

To configure the federated enterprises’ CMA systems to support federated H.323 calls:

1 See the *Polycom CMA System Operations Guide* for detailed information about adding a neighbored gatekeeper. Then go to Admin > Gatekeeper Settings > Neighboring Gatekeepers and add the RealPresence Access Director system as neighboring gatekeeper.

2 Go to Admin > Server Settings > Network and enter the VBP-E’s LAN interface address as the IPv4 Default Gateway address.

3 Go to Admin > Dial Plan and Sites > Dial Rules and add a Prefix dial rule. Assign it a Routing Action of Route to a trusted neighbor.

4 Go to Trusted Neighbors and select the RealPresence Access Director system as a trusted neighbor.
Task 6 (Conditional): Configure the VBP-5300E System to Support Federated H.323 Calls

If a CMA system is the gatekeeper for the federated enterprise using the VBP-E access controller, perform this task. Otherwise, skip to Task 7 (Conditional): Configure the VBP-5300E System in Embedded Gatekeeper Mode to Support Federated H.323 Calls.

To configure the federated enterprise’s VBP-5300E systems to support federated calls when the CMA system is the gatekeeper:

1. See the Polycom VBP System Configuration Guide for detailed information about specifying H.323 settings. Then go to Configuration Menu> VoIP ALG > H.323.

2. Select Gatekeeper mode > LAN/Subscriber-side gatekeeper mode and enter the CMA system’s IP address as the LAN/Subscriber-side GK address.

Task 7 (Conditional): Configure the VBP-5300E System in Embedded Gatekeeper Mode to Support Federated H.323 Calls

If the VBP-E is both the access controller and gatekeeper for the federated enterprise or division, perform this task.

To configure the federated enterprises’ VBP-5300E systems to support federated calls when the CMA system is the gatekeeper:

1. See the Polycom VBP System Configuration Guide for detailed information about specifying H.323 settings. Then go to Configuration Menu> VoIP ALG > H.323.

2. Select Gatekeeper mode > LAN/Subscriber-side gatekeeper mode and enter the CMA system’s IP address as the LAN/Subscriber-side GK address.

Federation in a SIP Environment with Acme Packet

Refer to the Acme Packet® Net-Net Enterprise Session Director (ESD) documentation to support calls from federated divisions or enterprises with an Acme Packet Net-Net Enterprise Session Director system in their environment.
Verifying Deployment

Verifying Access Proxy
Verifying access proxy confirms the functionality and connectivity between the RealPresence Access Director system and the RealPresence Mobile system, and between the RealPresence Access Director system and the RealPresence Resource Manager system.

To verify access proxy:
1. On the RealPresence Mobile device, configure a WiFi network. For example, if the RealPresence Access Director public IP address is 192.168.11.175, make sure that the RealPresence Mobile system can access this address.
2. On the RealPresence Mobile device, configure this sign-in setting.
   - **Provision Server**: FQDN or public IP address of the RealPresence Access Director system.
   - **User Name**: User account login managed by the RealPresence Resource Manager system.
   - **Password**: Correct password associated with User Name.
3. Click **Sign in**, and verify that sign-in was successful.
4. On the RealPresence Resource Manager system, go to **ENDPOINT > Monitor view** to check the status of the user.

Verifying Call Success

To verify registration and call success with the RealPresence DMA system:
1. Have a user sign into the RealPresence DMA system and verify that the user registered to the DMA system successfully.
2. Place a call, and verify that the call was established successfully.
3. Place a long call, and verify that the call remained connected.
4. Have the user sign out, and verify that the user was unregistered from the RealPresence DMA system successfully.

Verifying Certificates
Verifying certificates confirms that the administrator installed the correct certificates on the RealPresence Resource Manager, RealPresence Access Director, and RealPresence Mobile systems.
To verify certificates:

1. In the access proxy configuration, select these settings:
   - Require client certificate from the remote endpoint
   - Verify certificate from internal server

2. Have a user sign on to the RealPresence Mobile device, and verify that the user signed on successfully.

3. In SIP settings, select **TLS transport**, and verify that the user can register and place a call successfully.
Required Ports

This section describes the specific ports or dynamic port ranges to configure on your Polycom® RealPresence® Access Director™ system and correspondingly on your firewall. The port information is organized based on the different functions, or services, that the RealPresence Access Director system supports.

The dynamic source and destination port ranges listed here specify the allowable port ranges for communication between the RealPresence Access Director system and other systems and devices inside or outside of your enterprise network. The actual port ranges for your system depend on the number of calls on your license.

A port range for a specific function (for example, LAN-side SIP signaling) 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 do so, the RealPresence Access Director system automatically calculates the end ranges based on the number of calls on your license. For instructions, see Configuring Port Ranges in the Polycom RealPresence Access Director System Administrator Guide.

Caution: Ports configured in the RealPresence Access Director system must match your firewall ports

The specific ports and port ranges configured 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.

The following sections define the required ports to configure for the different traffic types, services, and functions supported by the RealPresence Access Director system:

- Management Access
- SIP Signaling
- H.323 Signaling
- Access Proxy
- Media
- TURN Server
- High Availability
- Two-System Tunnel Communication
- Comparison of Two-box Tunnel Deployment and Standard Deployment Ports
Management Access

The RealPresence Access Director system provides a web-based user interface to access, configure, and manage the system. Polycom suggests that you enable one interface as the management interface, segregated from WAN-accessible traffic. For greater security, Polycom recommends that you enable SSH and web access to the RealPresence Access Director system management interface only from authorized network segments. We also recommend that you disable SSH and web access from the WAN by creating explicit deny rules for these traffic types. If you require the ability to manage the RealPresence Access Director system from the WAN, see the table in Management Access Ports for specific requirements.

To support certain functions in the RealPresence Access Director system, connectivity is required between the management interface and the following external systems (servers):

- Network Time Protocol (NTP)
- Syslog
- DNS
- Microsoft Active Directory
- SNMP
- Online Certificate Status Protocol (OCSP)

Management Access Ports

The following table lists the required ports and transport protocols to access the system’s web-based user interface and to establish connections between the RealPresence Access Director system and external services. The table also lists access information to manage the RealPresence Access Director system from the WAN, if desired.

Management Access Ports

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD system management IP address</td>
<td>60001–64000</td>
<td>TCP</td>
<td>IP address of the RealPresence Platform Director system</td>
<td>3333 (RealPresence Platform Director system, version 1.7.0)</td>
<td>Connection from the RPAD system to the RealPresence Platform Director system for RPAD system license communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9333 (RealPresence Platform Director system, version 1.7.1)</td>
<td></td>
</tr>
</tbody>
</table>
### Management Access Ports

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealPresence Platform Director system IP address</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system management IP address</td>
<td>8443</td>
<td>Connection from the Polycom RealPresence Platform Director system to the RPAD system for Polycom API communication</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>60001–64000</td>
<td>UDP or TCP¹</td>
<td>IP address of SNMP server</td>
<td>162¹</td>
<td>Connection from the RPAD system to the SNMP server (for sending Trap messages)</td>
</tr>
<tr>
<td>IP address of the host sending an SNMP request to the RPAD system</td>
<td>&gt;1023</td>
<td>UDP or TCP¹</td>
<td>RPAD system management IP address</td>
<td>161¹</td>
<td>Connection from the LAN SNMP server to the RPAD system (for monitoring)</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>123</td>
<td>UDP</td>
<td>IP address of external NTP server, if in use</td>
<td>123</td>
<td>Connection from the RPAD system to the public NTP server</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>60001–64000</td>
<td>TCP</td>
<td>IP address of the OCSP responder, if in use</td>
<td>8080, 80</td>
<td>Connection from the RPAD system to the public OCSP responder</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>60001–64000</td>
<td>UDP</td>
<td>IP address of the DNS server</td>
<td>53</td>
<td>Connection from the RPAD system to the DNS server</td>
</tr>
</tbody>
</table>
### Management Access Ports

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
</table>
| RPAD system management IP address | 60001–64000 | TCP | IP address of the LAN-based Microsoft Active Directory server, if in use | 389 | StartTLS encrypted or unencrypted (TCP) connection from the RPAD system to the LAN-based Microsoft Active Directory server  
**Note:** This connection is optional. |
| RPAD system management IP address | 60001–64000 | TLS | IP address of the LAN-based Microsoft Active Directory server, if in use | 636 | Encrypted connection from the RPAD system to the LAN-based Microsoft Active Directory server  
**Note:** This connection is optional. |
| RPAD system management IP address | 60001–64000 | UDP or TCP² | IP address of the syslog server, if in use | 514, 10514 | Connection from the RPAD system to the syslog server  
**Note:** This connection is optional. |
| IP address of the WAN-based PC using a browser to access the RPAD system web (management) user interface | Any | TCP | RPAD system public management IP address | 8443 | HTTPS connection from a WAN-based PC to the RPAD system’s web user interface used to manage the system  
**Note:** This connection is optional. |
The RealPresence Access Director system serves as a SIP back-to-back user agent (B2BUA) and operates between endpoints that use the SIP protocol. When a SIP video call takes place, the RealPresence Access Director system divides the communication channel into two call legs and mediates all SIP signaling between the endpoints, from call establishment to termination. SIP signaling can be used for remote, guest, B2B, and open-SIP calls, and to initiate content streaming with a Polycom® RealPresence® Content Sharing Suite system.

### Management Access Ports

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the host managing the RPAD system using SSH</td>
<td>Any</td>
<td>TCP</td>
<td>RPAD system public management IP address</td>
<td>22</td>
<td>Access to the command line interface (CLI) of the RPAD system using SSH</td>
</tr>
</tbody>
</table>

1. The SNMP protocol and DST port depend on the SNMP settings you configure in the RealPresence Access Director system user interface. See the Polycom RealPresence Access Director System Administrator Guide for details.

2. The protocol for syslog service depends on the remote syslog settings you configure in the RealPresence Access Director system user interface. See the Polycom RealPresence Access Director System Administrator Guide for details.

### SIP Signaling

The RealPresence Access Director system serves as a SIP back-to-back user agent (B2BUA) and operates between endpoints that use the SIP protocol. When a SIP video call takes place, the RealPresence Access Director system divides the communication channel into two call legs and mediates all SIP signaling between the endpoints, from call establishment to termination. SIP signaling can be used for remote, guest, B2B, and open-SIP calls, and to initiate content streaming with a Polycom® RealPresence® Content Sharing Suite system.

**Caution: Disable services that intercept and alter SIP messages**

If your firewall has a SIP function that enables it to intercept and alter SIP messaging (for example, SIP ALG), you must disable the service. If not disabled, the service may cause call failures due to rewriting of port or IP address information.
SIP WAN Ports

The following table lists the required ports and protocols for bidirectional SIP signaling between the WAN and the RealPresence Access Director system.

### SIP Signaling Ports for the WAN and RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of external SIP client</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system public signaling IP address</td>
<td>5060¹</td>
<td>SIP (TCP 5060) connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td></td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public signaling IP address</td>
<td>5060</td>
<td>SIP connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td></td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system public signaling IP address</td>
<td>5061²</td>
<td>SIP TLS (TCP 5061) connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>13001–15000</td>
<td>TCP</td>
<td>Public signaling IP address of the other SIP system</td>
<td>&gt;1023³</td>
<td>Outbound SIP call from the RPAD system to another system</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>5060¹</td>
<td>UDP</td>
<td>IP address of remote user SIP client</td>
<td>&gt;1023</td>
<td>Outbound SIP call from the RPAD system to the remote user’s SIP client</td>
</tr>
</tbody>
</table>

¹ 5060 is the default SIP external listening port on the RealPresence Access Director system. If you change this external port or add other SIP external listening ports on the RealPresence Access Director system, the ports must also be changed or added on the firewall.

² 5061 is the encrypted (TLS) SIP external listening port on the RealPresence Access Director system.

³ Outbound calls normally resolve to TCP or UDP 5060 or TCP 5061 but DNS SRV queries may indicate any TCP or UDP port >1023.
SIP LAN Ports

The following table lists the required ports and protocols for bidirectional SIP signaling between the LAN and the RealPresence Access Director system.

**SIP Signaling Ports for the LAN and RealPresence Access Director System**

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal signaling IP address</td>
<td>13001–15000</td>
<td>TCP</td>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>5060–5061¹</td>
<td>SIP (TCP 5060) and SIP TLS (TCP 5061) connection from the RPAD system to the LAN-based SIP registrar (DMA system)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>5070²</td>
<td>UDP</td>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>5060¹</td>
<td>Connection from the RPAD system to the LAN-based SIP registrar (DMA system)</td>
</tr>
<tr>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>5060¹</td>
<td>UDP</td>
<td>RPAD system internal signaling IP address</td>
<td>5070²</td>
<td>Connection from the LAN-based SIP registrar (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>36000–61000</td>
<td>TCP</td>
<td>RPAD system internal signaling IP address</td>
<td>5070–5071²</td>
<td>SIP (TCP 5070) and SIP TLS (TCP 5071) connection from the LAN-based SIP registrar (DMA system) to the RPAD system</td>
</tr>
</tbody>
</table>

¹ 5060 and 5061 (encrypted TLS) are the default SIP listening ports on a RealPresence DMA system, so the RealPresence Access Director system ports must be the same as those on the RealPresence DMA system.
² 5070 and 5071 (encrypted TLS) are the default SIP internal listening ports on the RealPresence Access Director system. If you change these internal ports on the RealPresence Access Director system, they must be changed accordingly on your firewall.
H.323 Signaling

H.323 signaling enables registration, calling, and neighboring functions for endpoints that use the H.323 protocol. H.323 signaling can be used for remote, guest, and federated or neighbored B2B calls.

Caution: Disable services that intercept and alter H.323 messages

If your firewall has an H.323 function that enables it to intercept and alter H.323 messaging, for example, H.323 ALG, you must disable the service. If not disabled, the service may cause call failures due to rewriting of port or IP address information.

H.323 WAN Ports

The following table lists the required ports and protocols for H.323 signaling between the WAN and the RealPresence Access Director system.

H.323 Signaling Ports for the WAN and RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of external H.323 device</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public signaling IP address</td>
<td>1719&lt;sup&gt;2&lt;/sup&gt;</td>
<td>H.225 registration request from a remote endpoint to the RPAD system</td>
</tr>
<tr>
<td>Public signaling IP address of the other enterprise system</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public signaling IP address</td>
<td>1719</td>
<td>Inbound H.225 Location ReQuest (LRQ) to the RPAD system (suggested)</td>
</tr>
<tr>
<td>IP address of external H.323 device</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system public signaling IP address</td>
<td>1720&lt;sup&gt;3&lt;/sup&gt;</td>
<td>H.225 connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external H.323 device</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system public signaling IP address</td>
<td>10001–13000</td>
<td>H.245 connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of external H.323 device</td>
<td>1720</td>
<td>H.225 connection from the RPAD system to the WAN</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of external H.323 device</td>
<td>&gt;1023</td>
<td>H.245 connection from the RPAD system to the WAN</td>
</tr>
</tbody>
</table>
H.323 Signaling Ports for the LAN and RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD external signaling IP address</td>
<td>1719</td>
<td>UDP</td>
<td>Public signaling IP address of the other enterprise system</td>
<td>1719</td>
<td>H.225 gatekeeper neighboring connection from the RPAD system to the other enterprise system, if needed</td>
</tr>
</tbody>
</table>

1 The RealPresence Access Director system public signaling IP address refers to the public IP address for signaling mapped on the firewall located between the WAN and the RealPresence Access Director system.
2 1719 is the default listening port on the RealPresence Access Director system used by remote H.323 endpoints to request registration.
3 1720 is the default H.225 TCP port in the RealPresence Access Director system. If you change the port in the RealPresence Access Director system, you must also change it accordingly on the firewall.

H.323 LAN Ports

The following table lists the required ports and protocols for H.323 signaling between the LAN and the RealPresence Access Director system.

H.323 Signaling Ports for the LAN and RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal signaling IP address</td>
<td>1719¹</td>
<td>UDP</td>
<td>IP address of LAN-based H.323 gatekeeper (DMA system)</td>
<td>1719²</td>
<td>H.225 RAS connection for H.323 remote user registrations from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>1719</td>
<td>UDP</td>
<td>IP address of LAN-based H.323 gatekeeper (DMA system)</td>
<td>1719</td>
<td>H.225 gatekeeper neighboring connection from the RPAD system to the LAN-based H.323 gatekeeper (DMA system), if needed</td>
</tr>
</tbody>
</table>
### H.323 Signaling Ports for the LAN and RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 gatekeeper (DMA system)</td>
<td>1720²</td>
<td>H.225 connection from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 device</td>
<td>1720</td>
<td>H.225 connection from the RPAD system to the LAN-based H.323 device (with the DMA system in Direct mode)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 gatekeeper (DMA system)</td>
<td>36000–61000³</td>
<td>H.245 connection from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>10001–13000</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 device</td>
<td>&gt;1023</td>
<td>H.245 connection from the RPAD system to a LAN-based H.323 device</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>1719¹</td>
<td>UDP</td>
<td>RPAD system internal signaling IP address</td>
<td>1719</td>
<td>H.225 RAS connection from the LAN-based H.323 gatekeeper (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 device</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD system internal signaling IP address</td>
<td>1720</td>
<td>H.225 connection from the LAN-based H.323 device to the RPAD system (with the DMA system in Direct mode)</td>
</tr>
</tbody>
</table>
The RealPresence Access Director system access proxy feature provides reverse proxy services for external users. Based on your system configuration, when access proxy receives a request from an external user, it accepts the request and sends a new request on behalf of the user to the appropriate application server.

Access proxy routes communication requests based on the type of target application server:

- **HTTPS_proxy**: HTTPS servers that provide management services, such as provisioning for the RealPresence Access Director system and endpoints (Polycom® RealPresence® Resource Manager system, Polycom® RealPresence® Content Sharing Suite), and web-based video conferencing services (RealPresence CloudAXIS suite)

- **LDAP_proxy**: LDAP servers that provide directory services for remote (authorized) users
- **XMPP_proxy**: XMPP servers that provide message, presence, or other XMPP services for remote (authorized) users

- **HTTP tunnel proxy**: An HTTP tunnel proxy enables RealPresence CloudAXIS suite SIP guest users to attend video conferences in an enterprise’s CloudAXIS suite Experience Portal. Due to restrictive firewall rules, if a CloudAXIS suite client cannot establish a native SIP/RTP connection to a 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 guest 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.

### Access Proxy WAN Ports

The following table lists the ports and protocols for access proxy traffic between the WAN and the RealPresence Access Director system.

#### Access Proxy Ports for the WAN and the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of external client</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>443(^1)</td>
<td>HTTPS connection from the WAN to the RPAD system to sign in for provisioning</td>
</tr>
<tr>
<td>IP address of external client</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>389(^1)</td>
<td>TLS-encrypted or unencrypted encrypted (TCP) LDAP connection from the WAN to the RPAD system(^2)</td>
</tr>
<tr>
<td>IP address of external client</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>5222</td>
<td>XMPP connection from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external RealPresence CloudAXIS suite browser client that signs into the CloudAXIS suite Experience Portal and/or the Services Portal(^2)</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>443</td>
<td>HTTPS web connection from the WAN to the RPAD system. The RPAD system can proxy to both the RealPresence CloudAXIS suite Experience Portal and Services Portal(^2)</td>
</tr>
</tbody>
</table>
### Access Proxy Ports for the WAN and the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of Polycom® RealPresence® Content Sharing Suite user</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>443</td>
<td>HTTPS connection from the WAN to the RPAD system. The RPAD system proxies connections from external RealPresence Content Sharing Suite users to the Content Sharing Suite server.</td>
</tr>
<tr>
<td>IP address of RealPresence CloudAXIS suite client using an HTTP tunnel proxy.</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system</td>
<td>443</td>
<td>HTTP tunnel proxy connection from the WAN to the RPAD system. The RPAD system terminates the tunnel and proxies the traffic to the internal systems. ³</td>
</tr>
</tbody>
</table>
**Access Proxy Ports for the WAN and the RealPresence Access Director System**

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of RealPresence Mobile client using an HTTP tunnel proxy</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>Public IP address of the RPAD system's external access proxy IP address</td>
<td>443</td>
<td>HTTPS tunnel proxy connection from the WAN to the RPAD system. The RPAD system terminates the tunnel and proxies the traffic to the internal systems.</td>
</tr>
</tbody>
</table>

1. 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.
2. The RealPresence Access Director system denies all unencrypted LDAP requests if you enable Enforce TLS for LDAP connection in the web user interface (Admin > Security Settings).
3. Access to the RealPresence CloudAXIS suite Services Portal is required only for users who create and host conferences, and who are typically members of your organization. Providing external guests direct access to the Services Portal is left to the administrator's discretion.
Access Proxy LAN Ports

The following table lists the ports and protocols for bidirectional access proxy traffic between the RealPresence Access Director system and the LAN.

### Access Proxy Ports for the LAN and the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>60001–64000</td>
<td>TCP</td>
<td>IP address of the LAN-based provisioning server that provisions the RPAD system</td>
<td>443</td>
<td>HTTPS connection from the RPAD system to the LAN-based provisioning server that provisions the RPAD system. <strong>Note:</strong> This connection is optional.</td>
</tr>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>30001–60000</td>
<td>TCP</td>
<td>IP address of the LAN-based management server that provisions the endpoints</td>
<td>443</td>
<td>HTTPS connection from the RPAD system to the LAN-based management server that provisions the endpoints.</td>
</tr>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>30001–60000</td>
<td>TCP</td>
<td>IP address of the LAN-based LDAP server</td>
<td>389</td>
<td>LDAP connection from the RPAD system to the LAN-based LDAP server.</td>
</tr>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>30001–60000</td>
<td>TCP</td>
<td>IP address of the LAN-based XMPP server</td>
<td>5222</td>
<td>XMPP connection from the RPAD system to the LAN-based XMPP server.</td>
</tr>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>30001–60000</td>
<td>TCP</td>
<td>IP address of the RealPresence CloudAXIS suite Services Portal and/or Experience Portal</td>
<td>443</td>
<td>HTTPS connection from the RPAD system to the RealPresence CloudAXIS suite Experience Portal and/or Services Portal.</td>
</tr>
</tbody>
</table>
The RealPresence Access Director system enables media traffic (audio, video, and content) to traverse the firewall during video conferencing calls.

**Media WAN Ports**

The following table lists the ports and protocols for bidirectional media relay between the WAN and the RealPresence Access Director system.

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal access proxy IP address</td>
<td>30001–60000</td>
<td>TCP</td>
<td>IP address of the Polycom® RealPresence® Content Sharing Suite server</td>
<td>443</td>
<td>HTTPS connection from the RPAD system to the RealPresence Content Sharing Suite server.</td>
</tr>
<tr>
<td>IP address of external device</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public media IP address</td>
<td>20002–30001</td>
<td>Inbound media (RTP) traffic from the WAN to the RPAD system.</td>
</tr>
<tr>
<td>RPAD system public media IP address</td>
<td>20002–30001</td>
<td>UDP</td>
<td>Public media IP address of the external device</td>
<td>&gt;1023</td>
<td>Outbound media traffic from the RPAD system to the to WAN.</td>
</tr>
</tbody>
</table>

1 The RealPresence Access Director system public media IP address refers to the public IP address for media mapped on the firewall located between the WAN and the RealPresence Access Director system.

2 Most firewalls do not require a specific policy for the outbound media port range. The port range is the same for both inbound and outbound media traffic. The port information is included here for reference.
Media LAN Ports

The following table lists the ports and protocols for bidirectional media traffic between the LAN and the RealPresence Access Director system.

### Media Ports for the LAN and the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD internal media IP address</td>
<td>40002–50001</td>
<td>UDP</td>
<td>Any LAN-based video conferencing device</td>
<td>&gt;1023</td>
<td>Inbound media traffic from the RPAD system to the LAN-based video device</td>
</tr>
<tr>
<td>IP address of the LAN-based video conferencing device</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system internal media IP address</td>
<td>40002–50001</td>
<td>Outbound media traffic from the LAN-based video conferencing device to the RPAD system</td>
</tr>
<tr>
<td>RPAD internal media IP address</td>
<td>16001–17000</td>
<td>TCP</td>
<td>IP address of LAN-based RealPresence Collaboration Server (RMX)</td>
<td>&gt;1023</td>
<td>Inbound BFCP content from the RPAD system to the LAN-based RealPresence Collaboration Server (RMX)</td>
</tr>
<tr>
<td>IP address of LAN-based RealPresence Collaboration Server (RMX)</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD internal media IP address</td>
<td>16001–17000</td>
<td>Outbound BFCP content from the LAN-based RealPresence Collaboration Server (RMX) to the RPAD system</td>
</tr>
</tbody>
</table>

1 By default, video devices choose a port greater than 1023 to receive media traffic from the RPAD system (far end). Most video devices allow you to limit the port range they use by specifying fixed ports. The destination port can be restricted if endpoints and bridges are using restricted inbound port ranges.

### TURN Server

The RealPresence Access Director system can act as a TURN server to enable firewall and NAT traversal of UDP media traffic between WebRTC-enabled clients.
## TURN Relay Ports

The following table lists the ports and protocols for bidirectional media relay between WAN and LAN WebRTC-enabled clients and the RealPresence Access Director system TURN server.

### TURN Ports for WAN and LAN-based WebRTC Endpoints and the TURN Server

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of internal or external WebRTC client</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public signaling IP address(^1)</td>
<td>65370-65379 Default: 3478</td>
<td>TURN allocation requests from an internal or external WebRTC client to the TURN server. This port is used only to establish a TURN session.</td>
</tr>
<tr>
<td>RPAD system public signaling IP address</td>
<td>65370-65379 Default: 3478</td>
<td>UDP</td>
<td>IP address of internal or external WebRTC client</td>
<td>&gt;1023</td>
<td>Allocation response from the TURN server to an internal or external WebRTC client. The response establishes the TURN session.</td>
</tr>
<tr>
<td>IP address of internal or external WebRTC client</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD system public signaling IP address</td>
<td>32768–65535 (Default range: 49152-65535)</td>
<td>Inbound media traffic from an internal or external WebRTC client to the TURN server.</td>
</tr>
<tr>
<td>RPAD system public signaling IP address</td>
<td>32768–65535 (Default range: 49152-65535)</td>
<td>UDP</td>
<td>IP address of internal or external WebRTC client</td>
<td>&gt;1023</td>
<td>Outbound media traffic relay from the TURN server to an internal or external WebRTC client</td>
</tr>
</tbody>
</table>

\(^1\) The RealPresence Access Director system public signaling IP address refers to the public IP address for signaling mapped on the firewall between the WAN and the RealPresence Access Director system.
High Availability

For the High Availability solution, you must map public IP addresses on your firewall to specific virtual or physical IP addresses on both RealPresence Access Director systems. For details, see Firewall Configuration in Deploying RealPresence Access Director Systems with High Availability.

The following table lists the ports and protocols used for internal communication between two RealPresence Access Director systems configured for High Availability.

![High Availability ports used for encrypted traffic between the two systems do not need to be open on the firewall]

If your High Availability configuration does not include at least one direct link, the two RealPresence Access Director systems use the High Availability ports to send and receive communication between the two systems. These ports do not need to be open on the firewall.

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address for each RPAD system</td>
<td>65011-65012</td>
<td>TCP, UDP</td>
<td>IP address for each RPAD system</td>
<td>65011-65012</td>
<td>Encrypted traffic between the two RPAD systems. Note: These ports do not need to be open on the firewall.</td>
</tr>
</tbody>
</table>

1 Communication between the two systems configured for High Availability must be routable if the systems do not have a direct link.

Two-System Tunnel Communication

If you deploy two RealPresence Access Director systems in a tunnel configuration, one system acts as the tunnel server and the other system as the tunnel client. Communication for the RealPresence Access Director system services is tunneled between the two servers.

In a tunnel configuration, signaling, access proxy, and media traffic travels through a secure tunnel connection between the tunnel client and tunnel server. Port 1194 for UDP tunnel communication does not need to be open on the firewall between the tunnel server and the tunnel client.

When you enable the tunnel feature on the tunnel server, the tunnel port is opened and 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 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, a secure tunnel connection exists between the tunnel server and tunnel client. This connection enables continued communication between the two systems.
Management traffic does not traverse the tunnel. Regardless of how you configure your management interface, you must ensure that your RealPresence Access Director system has access to all management functions described in Management Access.

The following table lists the port and protocol for traffic between a RealPresence Access Director system tunnel server and tunnel client.

**Tunnel Server and Tunnel Client Port and Protocol**

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD tunnel client IP address</td>
<td>1194&lt;sup&gt;1&lt;/sup&gt;</td>
<td>UDP</td>
<td>RPAD tunnel server IP address</td>
<td>1194&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Tunnel connection between the RPAD tunnel client and the RPAD tunnel server</td>
</tr>
</tbody>
</table>

<sup>1</sup> 1194 is the default port for the RealPresence Access Director system local tunnel server and tunnel client.

### Comparison of Two-box Tunnel Deployment and Standard Deployment Ports

The following tables describe port similarities and differences in a RealPresence Access Director system standard deployment and a two-server tunnel deployment.

**WAN and Tunnel Server Connections**

<table>
<thead>
<tr>
<th>From the WAN to the Tunnel Server</th>
<th>From the Tunnel Server to the WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Ports</strong></td>
<td><strong>Management Ports</strong></td>
</tr>
<tr>
<td>• The port range is the same for two-box tunnel and standard deployments (see Management Access Ports).</td>
<td>• The port range is the same for two-box tunnel and standard deployments (see Management Access Ports).</td>
</tr>
<tr>
<td><strong>H323 Ports</strong></td>
<td><strong>H323 Ports</strong></td>
</tr>
<tr>
<td>• The port range is the same for two-box tunnel and standard deployments (see H.323 WAN Ports).</td>
<td>• The port range is the same for two-box tunnel and standard deployments (see H.323 WAN Ports).</td>
</tr>
<tr>
<td><strong>SIP Ports</strong></td>
<td><strong>SIP Ports</strong></td>
</tr>
<tr>
<td>• The port range is the same for two-box tunnel and standard deployments (see SIP WAN Ports).</td>
<td>• The port range is the same for two-box tunnel and standard deployments (see SIP WAN Ports).</td>
</tr>
</tbody>
</table>
### LAN and Tunnel Client Connections

<table>
<thead>
<tr>
<th>From the LAN to the Tunnel Client</th>
<th>From the Tunnel Client to the LAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Ports</strong></td>
<td><strong>Management Ports</strong></td>
</tr>
<tr>
<td>• The port range is the same for two-box tunnel and standard deployments (see Management Access Ports).</td>
<td>• The port range is the same for two-box tunnel and standard deployments (see Management Access Ports).</td>
</tr>
<tr>
<td><strong>Tunnel Port</strong></td>
<td><strong>Tunnel Port</strong></td>
</tr>
<tr>
<td>• The default port is 1194 (see Two-System Tunnel Communication).</td>
<td>• The default port is 1194 (see Two-System Tunnel Communication).</td>
</tr>
</tbody>
</table>
Network Interface Configurations

This chapter provides illustrations and network interface configuration details for the different RealPresence Access Director system deployment models.

- Single Firewall Deployment with One Network Interface
- DMZ Deployment with One or More Network Interfaces
- Two-System Tunnel Deployment
- High Availability Deployment

Single Firewall Deployment with One Network Interface

The RealPresence Access Director system with one network interface card (NIC) is deployed at the DMZ of the single outside firewall. All traffic use one network interface and IP address.
All communication services are configured for one network interface card and IP address, as shown in the following table.

<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TURN</td>
</tr>
</tbody>
</table>

**DMZ Deployment with One or More Network Interfaces**

The RealPresence Access Director system can be deployed in the DMZ with either a standard configuration or a WAN/LAN configuration.

*Note: Polycom recommends the use of four network interfaces*

As a best practice, Polycom recommends that you configure IP addresses for all four network interface cards. This configuration is required in order to support media throughput greater than 256 MB.

The figure below shows deployment in the enterprise DMZ, between an inside and outside firewall.

**Standard Configuration**

In a standard configuration with 1–4 configured NICs, all network interface IP addresses must be within the same subnet. External signaling and access proxy must be assigned to the same interface. External signaling and access proxy, and external media must have NATed IP addresses on the external, WAN-side firewall. All other network interfaces route traffic to and from the enterprise LAN through the inside firewall without NAT.
The following table lists the recommended network interface settings for the different communication services in a standard configuration, based on the number of network interfaces you use.

<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</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></td>
<td></td>
<td>TURN</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</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></td>
<td>eth1</td>
<td>Management</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></td>
<td>TURN</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></td>
<td>eth2</td>
<td>Management</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></td>
<td>TURN</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>

**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.

<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&lt;br&gt;Internal SIP/H.323 signaling and access proxy&lt;br&gt;Internal media</td>
</tr>
<tr>
<td>Minimal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>implementation</td>
<td>eth1</td>
<td>External SIP/H.323 signaling and access proxy&lt;br&gt;External media&lt;br&gt;TURN</td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy&lt;br&gt;External media&lt;br&gt;TURN</td>
</tr>
<tr>
<td>Best practice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for</td>
<td>eth1</td>
<td>Internal SIP/H.323 signaling and access proxy&lt;br&gt;Internal media</td>
</tr>
<tr>
<td>implementation</td>
<td>eth2</td>
<td>Management</td>
</tr>
<tr>
<td>with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>segregated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy&lt;br&gt;TURN</td>
</tr>
<tr>
<td>Best practice</td>
<td>eth1</td>
<td></td>
</tr>
<tr>
<td>required to</td>
<td>eth2</td>
<td></td>
</tr>
<tr>
<td>support</td>
<td>eth3</td>
<td></td>
</tr>
<tr>
<td>media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>throughput</td>
<td></td>
<td></td>
</tr>
<tr>
<td>greater than</td>
<td>Internal SIP/H.323 signaling and access proxy&lt;br&gt;Management</td>
<td></td>
</tr>
<tr>
<td>256 MB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Two-System Tunnel Deployment**

In a two-system tunnel deployment, two RealPresence Access Director systems can be deployed to tunnel traffic to and from the inside network. In this model, one system with one to four network interfaces is deployed in the corporate back-to-back DMZ and acts as the tunnel server. The other system with one to three network interfaces is deployed behind the inside firewall and acts as the tunnel client.

The following figure illustrates a two-system tunnel deployment.
Tunnel Server Network Interface Configuration

The following table lists the recommended tunnel server network interface settings for RealPresence Access Director system external network traffic, tunnel communication, and management traffic.

<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>External signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>External signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>External signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>Management</td>
</tr>
<tr>
<td>4</td>
<td>eth0</td>
<td>External signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td>eth3</td>
<td>Management</td>
</tr>
</tbody>
</table>

Tunnel Client Network Interface Configuration

The following table lists the recommended tunnel client network interface settings for RealPresence Access Director system internal network traffic, tunnel communication, and management traffic.

<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>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal media</td>
</tr>
</tbody>
</table>
The settings you configure for your network depend on various factors, including your network architecture and policies. The following table provides two possible options for configuring the network interfaces on each of your RealPresence Access Director systems to support High Availability. These options may or may not be suitable within your own network environment.

<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, Internal signaling and access proxy, Internal media, Internal access proxy</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>Internal signaling and access proxy, Internal media</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>Management</td>
</tr>
</tbody>
</table>

### High Availability Deployment

The settings you configure for your network depend on various factors, including your network architecture and policies. The following table provides two possible options for configuring the network interfaces on each of your RealPresence Access Director systems to support High Availability. These options may or may not be suitable within your own network environment.

<table>
<thead>
<tr>
<th>Number of NICs</th>
<th>Name of Interface</th>
<th>Assigned Services Option 1</th>
<th>Assigned Services Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>eth0</td>
<td>External SIP/H.323 signaling and access proxy, Internal SIP/H.323 signaling and access proxy, External media, Internal media, Management, TURN, High Availability</td>
<td>NA</td>
</tr>
<tr>
<td>Number of NICs</td>
<td>Name of Interface</td>
<td>Assigned Services Option 1</td>
<td>Assigned Services Option 2</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>Management High Availability</td>
<td>Management High Availability External SIP/H.323 signaling and access proxy Internal SIP/H.323 signaling and access proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External SIP/H.323 signaling and access proxy Internal SIP/H.323 signaling and access proxy External media Internal media TURN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>Internal SIP/H.323 signaling and access proxy Internal media Management</td>
<td>Management High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External SIP/H.323 signaling and access proxy Internal SIP/H.323 signaling and access proxy External media TURN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>High Availability</td>
<td>External media Internal media</td>
</tr>
<tr>
<td>4</td>
<td>eth0</td>
<td>Management High Availability</td>
<td>Internal SIP/H.323 signaling and access proxy Internal media Management</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External SIP/H.323 signaling and access proxy Internal SIP/H.323 signaling and access proxy External media TURN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>External media</td>
<td>High Availability</td>
</tr>
<tr>
<td></td>
<td>eth3</td>
<td>Internal media</td>
<td>High Availability</td>
</tr>
</tbody>
</table>