Deploying Polycom® Unified Communications in RealPresence® Access Director™ System Environments
Trademark Information

Polycom® and the names and marks associated with Polycom’s products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries. All other trademarks are the property of their respective owners.

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

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

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

The EULA for your version is available on the Polycom Support page for the Polycom RealPresence Access Director system.

© 2012-2013 Polycom, Inc. All rights reserved.
Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA
No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc. Under the law, reproducing includes translating into another language or format.

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

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

This guide describes the Polycom® RealPresence® Access Director™ system 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, model, and user scenarios.

Related Documentation

This guide is meant to supplement the associated product documentation, not replace it. When deploying the systems in this solution, please have the product documentation accessible, specifically:

- Polycom RealPresence Access Director System Release Notes
- Polycom RealPresence Access Director System Getting Started Guide
- Polycom RealPresence Access Director System Administrator’s 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
- Polycom RealPresence Resource Manager System Operations Guide
- Polycom RealPresence Collaboration Server System Administrator’s Guide

Required Skills

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.
Contents

About This Guide ................................................... iii
  Related Documentation ........................................ iii
  Required Skills ................................................ iii

1 Unified Communications with the Polycom® RealPresence®
Access Director™ System Solutions ............................... 1
  Overview of the Polycom RealPresence Access Director System Solution . 2
  RealPresence Access Director System Solution Deployment Models . . . . 4
    Deployment with One Firewall and a Single Network Interface . . . . . 5
    Deployment in a DMZ Environment with One or More Network Interfaces ........................................... 5
    Deployment in a Tunnel Environment .......................................... 6
  Other Deployment Models ............................................ 6
  Supported Call Scenarios ........................................... 7
    Connecting Remote Users to the Enterprise (SIP and H.323) ........... 7
    Connecting Guest Users to the Enterprise (H.323 and SIP) ............. 7
    Connecting Trusted Divisions or Enterprises (H.323 and SIP) ........ 8
  Products Tested in this Solution .................................... 8

2 Deploying the RealPresence Access Director System in a
Corporate DMZ Environment ...................................... 11
  Configure the DNS Service ....................................... 12
  Configure Firewalls and Ports ................................... 15
  Install and Configure the RealPresence Access Director System ........ 16
  Configure the RealPresence Resource Manager System ................ 17
  Configure the RealPresence Access Director System ................... 21
  Configure the Polycom RealPresence DMA System .................... 23
  Configure Polycom Endpoint Systems ................................ 26
  Configure the Polycom RealPresence Collaboration Server ............. 27
  Configure the Polycom RSS™ System ................................ 27


3 Deploying Two RealPresence Access Director Systems in a Tunnel Environment ........................................ 29
   Configure the DNS Service for the Tunnel ................... 30
   Configure Firewalls and Ports .................................. 30
   Install and Configure the RealPresence Access Director Systems .................. 31
   Configure the RealPresence Resource Manager System .................... 38
   Configure the Polycom RealPresence DMA System .................. 38
   Configure Additional Polycom Components ..................... 39

4 Federation Between RealPresence Access Director Systems Only ...................................................... 41
   Federation in a SIP Environment .............................. 41
   Federation in an H.323 Environment ......................... 44

5 Federation Between RealPresence Access Director and Other Systems ............................................. 47
   Federation in an H.323 Environment with Polycom VBP-E Systems ........ 47
   Federation in a SIP Environment with Acme Packet ............ 51

6 Verifying Deployment ............................................. 55
   Verifying Access Proxy ............................................. 55
   Verifying Call Success ............................................. 55
   Verifying Certificates ............................................. 56

A Required Ports .................................................... 57
   Management Ports .................................................... 58
      From the WAN to the RealPresence Access Director System .......... 58
      From the LAN to the RealPresence Access Director System .......... 59
      From the RealPresence Access Director System to the WAN .......... 59
      From the RealPresence Access Director System to the LAN .......... 60
   H.323 and WAN Ports .................................................. 61
      From the WAN to the RealPresence Access Director System .......... 61
      From the RealPresence Access Director System to the WAN .......... 62
      From the WAN to the RealPresence Access Director System: H.323 B2B Calls ........................................... 62
      From the RealPresence Access Director System to the WAN: H.323 B2B Calls ........................................... 63
   H.323 and LAN Ports .................................................... 64
      From the RealPresence Access Director System to the LAN .......... 64
From the LAN to the RealPresence Access Director System .......... 65
From the RealPresence Access Director System to the LAN: H.323 B2B Calls .................................................. 66
From the LAN to the RealPresence Access Director System: H.323 B2B Calls ........................................... 67
SIP and WAN Ports ...................................................... 67
From the WAN to the RealPresence Access Director System ....... 68
From the RealPresence Access Director System to the WAN ...... 69
SIP and LAN Ports .......................................................... 69
From the RealPresence Access Director System to the LAN ...... 69
From the LAN to the RealPresence Access Director System ...... 71
Tunnel Communication Ports ............................................ 72
From the RealPresence Access Director System Tunnel Server (DMZ) to the Tunnel Client (LAN) ...................... 72
From the RealPresence Access Director System Tunnel Client (LAN) to the Tunnel Server (DMZ) .................... 72
Comparison of Tunnel Deployment and Standard Deployment Ports ... 73
From the WAN to the RealPresence Access Director System and the RealPresence Access Director System to the WAN, .................. 73
From the LAN to the RealPresence Access Director System and the RealPresence Access Director System to the LAN, .............. 73

B Network Interface Configurations .............................. 75
Single Firewall Deployment with One Network Interface .......... 75
DMZ Deployment with One or More Network Interfaces .......... 76
Two-system Tunnel Deployment ...................................... 77
Tunnel Server Network Interface Configuration .................... 78
Tunnel Client Network Interface Configuration .................... 79
Unified Communications with the Polycom® RealPresence® Access Director™ System Solutions

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 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 System Solution” on page 2
- “RealPresence Access Director System Solution Deployment Models” on page 4
- “Supported Call Scenarios” on page 7
- “Products Tested in this Solution” on page 8
Overview of the Polycom RealPresence Access Director System Solution

The Polycom video infrastructure integrates with the RealPresence Access Director system to provide video conferencing management for remote, guest, and federated users with secure firewall traversal for all 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 RealPresence Resource Manager system or RealPresence Content Sharing Suite (the latter supports video sharing among Lync conference participants).</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 server, and enables sending of outgoing XMPP signaling to other remote endpoints.</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 server.</td>
</tr>
<tr>
<td>TCP Reverse Proxy</td>
<td>Enables a TCP connection for Web clients to send meeting requests to the internal Meeting Experience Application (MEA) on a Polycom® RealPresence® CloudAXIS™ Suite server.</td>
</tr>
</tbody>
</table>
| SIP Signaling   | Enables:  
  • SIP signaling from remote users via designated video endpoints to traverse the firewall to the internal SIP server.  
  • Use of separate interfaces for external and internal SIP signaling messages  
  • Sending of outgoing SIP signaling to remote endpoints.  
  • Modifying SIP signaling to direct media through the media relay when required. |

Polycom RealPresence Access Director System Solution Deployment Guide
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| H.323 Signaling      | Enables:  
• H.323 signaling from and to remote users via designated video endpoints to traverse the firewall to the internal gatekeeper.  
• Use of separate interfaces for external and internal H.323 signaling messages  
• Functionality to understand and manipulate all H.323 Annex O dialing messages.  
• Functionality to route all H.323 messages from guest users to and from the internal gatekeeper. |
| Media Relay          | Enables media from remote and guest users residing in federated sites to traverse the firewall. The media relay functions as an SBC-based relay.                                            |
| Static Routing       | 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 |
| H.460 Support        | 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 and NATs. |
| Access Control Lists | The RealPresence Access Director system supports the use of Access Control Lists for SIP and H.323 calls that come through the external signaling ports. Access Control List rules define whether the RealPresence Access Director system allows or denies a specific type of SIP or H.323 request from a public network, which provides increased protection against external security threats. |
| Configurable Port Ranges | The RealPresence Access Director system allows you to configure port range settings to decrease the number of dynamic ports that need to be open on your enterprise’s outside firewall. When you specify a beginning port range number for signaling or media dynamic source ports, the RealPresence Access Director system automatically calculates the end port number for that service based on the number of calls on your system license. |
In this solution, the RealPresence Access Director system uses access proxy to enable remote users to be provisioned and managed by setting up the HTTPS, LDAP, and XMPP connections with the RealPresence Resource Manager system. When access proxy receives an HTTPS, LDAP, or XMPP connection request from an external endpoint, the RealPresence Access Director system accepts the request and initializes a request to the internal HTTPS, LDAP, or XMPP server.

If your organization has implemented the RealPresence Access Director system as part of the Polycom RealPresence CloudAXIS Suite, access proxy supports a TCP connection that Web clients can use to send meeting requests to the internal Meeting Experience Application (MEA) on the CloudAXIS Suite server.

If your RealPresence Access Director system provides firewall traversal for a Polycom® RealPresence® Content Sharing Suite, HTTPS requests can be forwarded to the RealPresence Content Sharing Suite server.

If your system is deployed with both a RealPresence Resource Manager system and a RealPresence Content Sharing Suite server, the RealPresence Access Director system forwards requests to the correct server based on the access proxy HTTPS configuration settings. See the Polycom® RealPresence® Access Director™ System Administrator’s Guide for configuration details.

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” on page 5
- “Deployment in a DMZ Environment with One or More Network Interfaces” on page 5
- “Deployment in a Tunnel Environment” on page 6
• “Other Deployment Models” on page 6
See Appendix B 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, and management traffic use one network interface and IP address.

Deployment in a DMZ Environment with One or More Network Interfaces

In general, Polycom recommends that the RealPresence Access Director system be deployed in a corporate back-to-back DMZ; that is, deployed between an outside (also referred to as public or external) firewall and inside (also referred to as private or internal) firewall. Figure 1-1 illustrates a standard deployment.

*Figure 1-1  Polycom Unified Communications with the RealPresence Access Director System Standard Deployment*
In this implementation:

- The outside firewall, which resides between the WAN (Untrust) and the RealPresence Access Director system in the DMZ, 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 is recommended for the outside firewall.

- The inside firewall, which resides between the RealPresence Access Director system in the DMZ and the LAN (Trust), 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.

This approach 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 “two-legged” configuration. In this scenario, SIP and H.323 signaling and media traffic are split between the interfaces to separate external and internal traffic.

### Deployment in a Tunnel Environment

Two RealPresence Access Director systems can be deployed to tunnel traffic to and from the inside network. 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 this scenario, the tunnel server can forward all traffic through one open port on the inside firewall. If necessary, based on the firewall policy, the tunnel client can also send all traffic through one open port on the inside firewall.

### 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.
Supported Call Scenarios

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

- Connecting Remote Users to the Enterprise (SIP and H.323)
- Connecting Guest Users to the Enterprise (H.323 and SIP)
- Connecting Trusted Divisions or Enterprises (H.323 and SIP)

Connecting Remote Users to the Enterprise (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.

Connecting Guest Users to the Enterprise (H.323 and SIP)

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 site.
- Division or enterprise users can place H.323 video calls out to guest users.
- Division or enterprise users can place SIP calls out to guest users who are members of a federated site.

Appendix B includes diagrams and the recommended network interface configurations supported for this solution.
• Guest users do not have access to any management services such as endpoint provisioning, user directory, XMPP contact list and presence services, or SIP calling, calendaring, and scheduling services.

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

Connecting Trusted Divisions or Enterprises (H.323 and SIP)

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:
• Chapter 4, “Federation Between RealPresence Access Director Systems Only” on page 41.
• Chapter 5, “Federation Between RealPresence Access Director and Other Systems” on page 47.

Products Tested in this Solution

The following products are supported in this RealPresence Access Director system solution.

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Version</th>
<th>Function in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Access Director</td>
<td>3.0</td>
<td>Secures access to H.323 and SIP video services for small- to medium-sized federated enterprises.</td>
</tr>
<tr>
<td>Polycom RealPresence Distributed Media Application™ (DMA™) 7000</td>
<td>6.0.2</td>
<td>Functions as SIP proxy/registrar, H.323 gatekeeper, SIP and H.323 gateway, and bridge virtualizer.</td>
</tr>
<tr>
<td>Polycom Product</td>
<td>Version</td>
<td>Function in Solution</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polycom RealPresence Resource Manager</td>
<td>7.1.1</td>
<td>Provisions and manages remote endpoints, and enables directory and presence services.</td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td></td>
</tr>
<tr>
<td>Polycom RSS™ 4000</td>
<td>8.5</td>
<td>Provides recording functionality for video, audio, and content.</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server 1500, 2000, and 4000</td>
<td>7.8</td>
<td>Provides bridge capability for SIP and H.323 conferences, including support for content over video.</td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server 800s</td>
<td>7.8</td>
<td>Provides bridge capability for SIP and H.323 conferences, including support for content over video.</td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td></td>
</tr>
<tr>
<td>Polycom HDX Series</td>
<td>3.1.0</td>
<td>Video conferencing endpoint systems.</td>
</tr>
<tr>
<td></td>
<td>3.1.2</td>
<td></td>
</tr>
<tr>
<td>Polycom RealPresence Mobile</td>
<td>2.3</td>
<td>Serves as client application for supported Apple® devices.</td>
</tr>
<tr>
<td></td>
<td>3.0</td>
<td></td>
</tr>
<tr>
<td>Acme Packet Net-Net ESD</td>
<td>6.3</td>
<td>Testing was carried out specifically with the Acme Packet Net-Net ESD-3820 platform running S-Cx6.3.MF-2 software. Other Acme Packet E-SBCs such as Net-Net ESD-4500, Net-Net ESD-SE and Net-Net ESD-VME also run the same line of C-series software. These other products can also be used in this Polycom RealPresence solution.</td>
</tr>
<tr>
<td>Polycom Video Border Proxy (VBP)</td>
<td>11.2.16</td>
<td>In some solution models, provides border control functionality for federated enterprises.</td>
</tr>
<tr>
<td>Polycom CMA system</td>
<td>6.2</td>
<td>In those solution models using a Polycom VBP-E border controller, the CMA system is behind the VBP system and provides management and H.323 gatekeeper functionality.</td>
</tr>
<tr>
<td>Polycom RealPresence Group 300 and Group 500</td>
<td>4.1.0</td>
<td>Video conferencing endpoint systems.</td>
</tr>
<tr>
<td></td>
<td>4.1.1</td>
<td></td>
</tr>
</tbody>
</table>
Deploying the RealPresence Access Director System in a Corporate DMZ Environment

This chapter 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.
Polycom RealPresence Access Director System Solution Deployment Guide

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

- "Configure the DNS Service" on page 12
- "Configure Firewalls and Ports" on page 15
- "Install and Configure the RealPresence Access Director System" on page 16
- "Configure the RealPresence Resource Manager System" on page 17
- "Configure the RealPresence Access Director System" on page 21
- "Configure the Polycom RealPresence DMA System" on page 23
- "Configure SIP Settings for Registered and Guest Users" on page 24
- "Configure Polycom Endpoint Systems" on page 26
- "Configure the Polycom RealPresence Collaboration Server" on page 27
- "Configure the Polycom RSS™ System" on page 27

**Configure the DNS Service**

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

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 1**

**Create a DNS A record on the external DNS server**

Create a DNS A (address) record on the external DNS server to map the FQDN of the RealPresence Access Director system to its public IP address.

- So 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 IP address
Task 2 **Create a DNS SRV record on the external DNS server**

Create a DNS service record (SRV record) on the external DNS server to map the SRV service address for endpoint provisioning 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.

- If the RealPresence Access Director system has the FQDN name *rpad.example.com*, add an SRV record as follows.

  \[
  \_cmaconfig\_tcp.example.com. \text{IN} \text{SRV} 0 100 443 \text{ rpad.example.com}.
  \]

  Where:
  - **Service** = \_cmaconfig\_tcp
  - **Protocol** = \_tcp
  - **Priority** = 0
  - **Weight** = 100
  - **Port** = 443
  - **Host offering this service** = rpad.example.com

Task 3 **Create DNS A records on the internal DNS server**

Create three DNS A records on the internal DNS server as identified in the following sections.

The RealPresence Resource Manager system and the RealPresence DMA system in the internal network each need one A record to map their FQDNs to the IP address of the internal DNS server. In addition, the RealPresence Access Director system can use a specified FQDN as the provisioning server (access proxy configuration), SIP server, or gatekeeper (SBC setting). For example:

1. 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:

   \[
   \text{rprm.example.com IN A 10.22.202.134}
   \]

2. 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:

   \[
   \text{dma.example.com IN A 10.22.120.126}
   \]

3. 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:

   \[
   \text{rpad.example.com IN A 10.22.210.111}
   \]

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 `rpm.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 rpm.example.com.
```

The RealPresence DMA system requires several DNS SRV records on the internal DNS server to map the SRV service address for several services (SIP/TCP, SIP/UDP, and SIP/TLS) 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.
```

### Task 5

**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 6

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

Configure Firewalls and Ports

Follow these guidelines for configuring your firewalls and ports.

- 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 (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
- Disable the port NAT.
- Disable any H.323 helper services on the firewall (for example, Cisco® H.323 Fixup).

**Ports**

To enable firewall traversal for external clients, the RealPresence Access Director system uses ports for provisioning, presence, directory, call signaling, and media.

Outbound traffic from the RealPresence Access Director system uses 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 (up to 10 ports per session).

Incoming traffic from external clients uses static ports you define in the RealPresence Access Director system user interface. See the Polycom RealPresence Access Director System Administrator’s Guide.

For detailed information on required ports, refer to Appendix A.

# Install and Configure the RealPresence Access Director System

## Task 1  Perform Basic Installation

Perform the basic installation and network configuration as documented in the RealPresence Access Director System Getting Started Guide.

## Task 2  Set the Time Zone

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

1. Go to Admin > Time Settings > System time zone and select the time zone of your specific geographic location.

## Task 3  Activate the License

To activate the license for your system, you must obtain an activation key code from Polycom Support at support.Polycom.com.
To obtain an activation key code
1  Go to the Polycom Support site.
2  Enter the server’s serial number and the license number that you were given for that server.
   An activation key is generated for that server.

To activate a license
1  Go to Maintenance > License.
2  Enter the Activation key for the license and click Update.
   The system restarts.

Task 4  Configure Network Settings
You must configure the network settings for the RealPresence Access Director system based upon the deployment model you are implementing. For more information about the deployment models, see “RealPresence Access Director System Solution Deployment Models” on page 4. For more information about RealPresence Access Director system network settings, see the Polycom RealPresence Access Director Administrator’s Guide.

To configure the network settings
1  From your Web browser, enter the IP address of the RealPresence Access Director system and log into the user interface.
2  Go to Admin > Network Settings.
   The General Network Settings that display are the settings configured during initial installation and first-time setup of the system.
3  Click Advanced network settings > Configuration Wizard and configure the network interface settings, binds, and static route settings for the different services (external and internal signaling and access proxy, external and internal media, and management).

Configure the RealPresence Resource Manager System
The following sections assume that the RealPresence Resource Manager system is already installed and configured for use.
The tasks listed below describe the configuration steps to perform on version 7.1.1 of the RealPresence Resource Manager system to enable RealPresence Access Director system integration and provisioning:
•  Add a Site for the RealPresence Access Director System
• Add a Provisioning User Account for the RealPresence Access Director System
• Add a Provisioning User Account for Endpoints

For complete instructions on configuring the RealPresence Resource Manager system, see the Polycom RealPresence Resource Manager System Operations Guide for your version of the RealPresence Resource Manager system.

Task 1

Add a Site for the RealPresence Access Director System

The system secures a specific network segment or subnet. To accurately characterize and represent that network segment, you must create a site on the RealPresence Resource Manager system that is specifically enabled for the RealPresence Access Director system. Your remote users will be managed through this site.

Use the instructions below for version 7.1.1 of the RealPresence Resource Manager system. For later versions,

To add a site to the RealPresence Resource Manager system

1 See the Polycom RealPresence Resource Manager System Operations Guide for detailed information about adding a site. Then go to Admin > Topology > Sites and add a site.

2 On the General Info tab of the Add Site dialog box, select Site with RPAD. Complete the other fields of the tab as required.

3 On the Subnets tab, add a subnet. Enter the RealPresence Access Director system internal signalling IP address and Mask (255.255.255.255).

4 Complete the other tabs and fields of the Add Site dialog box as required and finish adding the site.

   The site is added to the system, and the Add Site Provisioning Details dialog box appears.

5 On the Directory Setting tab, enter the RealPresence Access Director system’s public IP address as Directory Server. Complete the other fields of the tab as required.

6 On the Presence Settings tab, enter the RealPresence Access Director system’s public IP address as Presence Server. Complete the other fields of the tab as required.
7 On the **RPAD Settings** tab, configure the general system values for the RealPresence Access Director system deployment.

8 On the **RPAD Settings** tab, enter the required values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP H.323</td>
<td>Select this if support for H.323 signalling is required for H.323 endpoints.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>In this solution, the RealPresence DMA system is the gatekeeper, so enter the RealPresence DMA system IP address here.</td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Select this if support for SIP signalling is required for SIP endpoints.</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>Enter the address of the internal SIP proxy server to which the RealPresence Access Director system forwards information when an endpoint sends SIP registration or SIP call routing. In this solution, the RealPresence DMA system is the proxy server, so this is the RealPresence DMA system IP address.</td>
</tr>
<tr>
<td>Registrar Server</td>
<td>Enter the public IP address or the DNS name of the RealPresence Access Director system.</td>
</tr>
<tr>
<td>Note</td>
<td>If using a custom port for remote users, enter the following text after the public IP address or DNS name: <code>&lt;custom port number&gt;</code></td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>Enter TCP as the SIP signal transport protocol. Polycom suggests using TCP but UDP, UDP/TCP, or TLS may also be used. You must specify the same protocol as the protocol used in the RealPresence Access Director system for remote users.</td>
</tr>
<tr>
<td>Verify Certificate (SIP Settings)</td>
<td>(SIP Settings) Indicate whether to verify certificate between the RealPresence Access Director system and the SIP server.</td>
</tr>
<tr>
<td>Use Default Directory Server</td>
<td>This server or specify a directory server.</td>
</tr>
<tr>
<td>Directory Server</td>
<td>Enter the address of the internal LDAP server to which the RealPresence Access Director system forwards information when an endpoint tries to register to an LDAP directory.</td>
</tr>
<tr>
<td>Verify Certificate (Directory Settings)</td>
<td>(Directory Settings) Indicate whether to verify certificate between the RealPresence Access Director system and LDAP server.</td>
</tr>
<tr>
<td>Use Default Presence Server</td>
<td>This server or specify a presence server.</td>
</tr>
<tr>
<td>Presence Server</td>
<td>Enter the address of the internal presence server to which the RealPresence Access Director system forwards information when an endpoint tries to register to a presence server.</td>
</tr>
<tr>
<td>Verify Certificate (Presence Settings)</td>
<td>(Presence Settings) Indicate whether to verify certificate between the RealPresence Access Director system and presence server.</td>
</tr>
</tbody>
</table>
To enable remote users with H.323 endpoints:

a  On the **H.323 Settings** tab, select **Enable IP H.323** and in the **Gatekeeper Address** field, enter the RealPresence Access Director system’s public IP address for H.323 signaling.

b  Complete the other fields of the tab as required.

To enable remote users with SIP endpoints:

a  On the **SIP Settings** tab, select **Enable SIP** and in the **Proxy Server** and **Registrar Server** fields, enter the RealPresence Access Director system’s public IP address for SIP signaling.

b  Set the **Transport Protocol** to TLS.

c  Complete the other fields of the tab as required.

Complete the other fields of the dialog box as required.

**Task 2**

**Add a Provisioning User Account for the RealPresence Access Director System**

To provision a RealPresence Access Director system, the RealPresence Resource Manager system must have a user account dedicated for this purpose. This user account is the Login Name and Password that you enter on the RealPresence Access Director system to enable the integration and provisioning capability.

Because this user account is for system authentication only, the account:

- Should not be a real user account
- Needs only the minimum required user information

**To add a provisioning user account to the RealPresence Resource Manager system for this purpose**

1  See the *Polycom RealPresence Resource Manager System Operations Guide* for detailed information about adding a user account. Then go to **User > Users > Add**.

2  On the **General Info** tab of the **Add New User** dialog box, enter the minimum required information, as indicated by an asterisk and then click **OK**.
Task 3  Add a Provisioning User Account for Endpoints

To provision endpoint systems through the firewall, the RealPresence Resource Manager system must have a user account dedicated for this purpose. This user account is the user name and password that you must enter on the endpoint system to enable the integration and provisioning capability.

To add a user account to the RealPresence Resource Manager system for an endpoint

1  See the Polycom RealPresence Resource Manager System Operations Guide for detailed information about adding a user account. Then go to User > Users > Add.

2  On the General Info tab of the Add New User dialog box, enter the minimum required information, as indicated by an asterisk and then click OK.

3  On the Dial String Reservations tab, enter the SIP URI for the endpoint and then click OK.

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.

The following sections describe the tasks to be performed. They include:

- Configure System Certificates
- Configure Automatic Provisioning (Recommended)

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

Task 1  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.

The RealPresence Access Director system certificate must be both a serverauth and clientauth certificate.

You should configure certificates before configuring automatic provisioning of the RealPresence Access Director system and before federating your RealPresence Access Director system with another enterprise. For more information about certificate signing requests and certificates, see the Polycom RealPresence Access Director Administrator’s Guide.
Task 2 Configure Automatic Provisioning (Recommended)

When integrated with a Polycom Management System, the RealPresence Access Director system connects to the RealPresence Resource Manager system to get some of the configuration information you entered when you configured the management system. (See “Configure the RealPresence Resource Manager System” on page 17.)

Specifically, automatic provisioning configures:

- An NTP server for system time
- Access proxy settings
- SIP and H.323 signaling settings

After connecting and enabling provisioning mode, you cannot update the provisioned information manually in the RealPresence Access Director system until after disconnecting.

To configure automatic provisioning on the RealPresence Access Director system

1. See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring automatic provisioning. Then go to Admin > Polycom Management System.

2. Enter the Login Name, Password, and RealPresence Resource Manager IP address for the RealPresence Access Director system provisioning user account, and then click Connect.

When the RealPresence Access Director system connects successfully to the RealPresence Resource Manager system, some SIP and H.323 settings are automatically provisioned.
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.

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.

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.

**IMPORTANT**  

If **Device Authentication** is enabled on the RealPresence DMA system, you must disable **Use Endpoint Provisioning Credentials** on the RealPresence Resource Manager system (see step 10 on page 20).

---

**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 “Add a Provisioning User Account for Endpoints” on page 21. 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**.

4. Clear **Device Authentication**.
Configure SIP Settings for Registered and Guest Users

To support SIP guest calls, additional settings must be configured on the RealPresence DMA system and on the RealPresence Access Director system. Polycom recommends the configurations described in the following sections:

- “Configure SIP settings for guests on the RealPresence DMA system” on page 24
- “Configure SIP settings for guest users on the RealPresence Access Director system” on page 25
- “Configure SIP settings for registered users on the RealPresence Access Director system” on page 26

Task 2

Configure SIP settings for guests on the RealPresence DMA system

Your RealPresence DMA system must be configured with a dial rule prefix that corresponds to the prefix used for guests 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 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 three dial rules to handle the incoming unauthorized guest calls; one for each type of call resolution:
   - Resolve to conference room ID
   - Resolve to virtual entry queue
   - Resolve to external SIP peer

5. Go to Admin > Call Server > Domains and add a domain to the domain list for the host specified for guest port configuration.
Task 3  Configure SIP settings for guest users on the RealPresence Access Director system

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

1  See the Polycom RealPresence Access Director Administrator’s 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.
   - The host is a domain name change the system can implement. 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 users 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 Administrator’s 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.
   - The host is a domain name change the system can implement. 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 users dial string to 778222@example.com.
Task 4 Configure SIP settings for registered users on the RealPresence Access Director system

If you configure the external SIP ports 5060 and 5061 for guest users, you must also add an external SIP port for registered users.

To configure a RealPresence Access Director system non-standard external SIP port to support registered 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. See “To add a site to the RealPresence Resource Manager system” on page 18.

Configure Polycom Endpoint Systems

This solution supports the Polycom endpoint systems identified in “Products Tested in this Solution” on page 8.

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 system 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.
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.

Configure the Polycom RSS™ System

Ensure that the Polycom RSS 4000 system is in normal mode, not maximum security mode.

Refer to the Polycom RSS 4000 User Guide for more information about Polycom RSS working modes.
Deploying Two RealPresence Access Director Systems in a Tunnel Environment

This chapter describes the configuration processes required for deploying two RealPresence Access Director systems to tunnel traffic to and from the inside network.

If you deploy two RealPresence Access Director systems in a tunnel configuration, one system acts as the tunnel server and the other system as the tunnel client. In a tunnel configuration, certain IP addresses are reserved for internal system use. The IP address you define for each system must differ from the IP addresses listed below:

- Non-encrypted tunnel: 192.168.99.21

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

Before enabling the tunnel feature, activate the licenses for both of the RealPresence Access Director systems.

See these topics for detailed information about tunnel configuration settings.

- “Configure the DNS Service for the Tunnel” on page 30
- “Configure Firewalls and Ports” on page 30
- “Install and Configure the RealPresence Access Director Systems” on page 31
- “Configure the RealPresence Resource Manager System” on page 38
- “Configure the Polycom RealPresence DMA System” on page 38
- “Configure Additional Polycom Components” on page 39
Configure the DNS Service for the Tunnel

Refer to “Deploying the RealPresence Access Director System in a Corporate DMZ Environment” on page 11 in this guide for complete DNS service configuration instructions.

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 Remote tunnel client address field in the tunnel server settings.

• Two network interfaces: The internal signal and media IP address of the tunnel client. This IP address matches the Internal signal and media IP 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.

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).

For more information on port configuration, refer to Appendix A.

Install and Configure the RealPresence Access Director Systems

Task 1 Perform Basic Installation

Perform the basic installation and network configuration of two RealPresence Access Director systems as documented in the RealPresence Access Director System Getting Started Guide.

Task 2 Synchronize the Time and Set the Time Zones

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

- Synchronize the time on the two systems (tunnel server and tunnel client) to the same Network Time Protocol (NTP) server before encrypting the tunnel (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 system that acts as 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.
5. Click Update and OK to accept your settings and restart the system.
6 Repeat the above steps for the system that acts as the tunnel client.

Changing the time settings requires a system restart.

Task 3

Activate the System Licenses

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. You must purchase and activate a license for each system. The license with the fewest number of calls reflects the total number of licensed calls available.

After activating both licenses, you can view the number of licensed calls from the user interface (Maintenance > License) 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 system that will act as 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 system that will act as 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

In a tunnel deployment, most network settings are configured on the RealPresence Access Director system that will act as the tunnel server, located in the corporate back-to-back DMZ. Network settings for the tunnel server can be configured for one to four network interfaces. Note that you must also assign a network interface for the tunnel itself. On the tunnel server, the network interface assigned to tunnel communication is the IP address of the remote tunnel client.
To configure network settings for the tunnel server

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

2. Go to Admin > Network Settings > General network setting.
   The General Network Settings that display are the settings configured for eth0 during initial installation and first-time setup of the system.

3. Revise the general settings if necessary. Fields marked with an asterisk (*) are required.

4. Click Advanced network setting > Configuration Wizard.

5. In the Step 1 of 2: Advanced Network Settings window, click each of the network interfaces to configure and complete the fields below:
   - IPv4 Address
   - IPv4 Subnet Mask
   - IPv4 Default Gateway

6. Click Next.

7. In the Step 2 of 2: Service Network Settings window, select the IP address of the network interface to assign to each type of traffic and to the tunnel (see the recommended network interface configurations in Appendix B, “Two-system Tunnel Deployment” on page 77):
   - External Signaling IP: The IP address of the network interface used for SIP and H.323 signaling and access proxy traffic between the RealPresence Access Director system and external networks.
   - External Relay IP: The IP address of the network interface used for media relay between the RealPresence Access Director system and external networks.
   - Management IP: The IP address of the network interface used for tunnel communication and management traffic, including Web management of the user interface, SSH, DNS, NTP, remote syslog, and OCSP.

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

   If you are using three or four network interfaces on the tunnel server, tunnel communication and management traffic may be assigned to different network interfaces. In this case, select the network interface used for management traffic in the Management IP field. Configure the interface for tunnel communication in the tunnel settings (see “Configure Tunnel Settings on the Tunnel Server” on page 35). On the tunnel server, the network interface assigned to tunnel communication is the IP address of the remote tunnel client.
— **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.

9 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 or two network interfaces. On the tunnel client, the network interface assigned to tunnel communication is the IP address of the remote tunnel server.

**To configure network settings for the tunnel client**

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

2 Go to **Admin > Network Settings > General network setting**.

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

3 Revise the general settings if necessary. Fields marked with an asterisk (*) are required.

4 Click **Advanced network setting > Configuration Wizard**.

5 In the **Step 1 of 2: Advanced Network Settings** window, click each of the network interfaces to configure and complete the fields below:

   – **IPv4 Address**
   – **IPv4 Subnet Mask**
   – **IPv4 Default Gateway**

6 Click **Next**.
7 In Step 2 of 2: Service Network Settings > Management IP, select the IP address of the network interface used for management traffic.

If the tunnel client uses only one network interface, the Management IP interface is also used for tunnel communication, internal signaling and internal media traffic.

To specify the network interface used for internal signaling and media traffic, configure the settings for the tunnel client (see “Configure Tunnel Settings on the Tunnel Client” on page 36).

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

9 Configure the tunnel settings on the tunnel client.

Task 6

Configure Tunnel Settings on the Tunnel Server

If you use the encryption option for the tunnel, you must first synchronize the time on the tunnel server and the tunnel client to the same Network Time Protocol (NTP) server before encrypting the tunnel. See “Synchronize the Time and Set the Time Zones” on page 31.

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

To configure settings on the tunnel server

1 Go to Configuration > Tunnel Settings.

2 Use the information in the table 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>Select to enable the tunnel feature.</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
</tr>
<tr>
<td>Server Client</td>
<td>Select Server to enable the system to operate as a tunnel server.</td>
</tr>
<tr>
<td>Encrypted tunnel</td>
<td>When selected, tunnel communications are encrypted.</td>
</tr>
<tr>
<td>Note</td>
<td>This setting must be the same on both the tunnel server and tunnel client.</td>
</tr>
</tbody>
</table>
Click Update.
The system restarts.

### Task 7

#### Configure Tunnel Settings on the Tunnel Client

To configure tunnel settings on the tunnel client

1. Go to Configuration > Tunnel Settings.

2. Use the information in the table 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>Performance profile</td>
<td>If tunnel encryption is enabled, select a performance profile.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The profiles on the tunnel server and client must match.</td>
</tr>
<tr>
<td><strong>Premium</strong></td>
<td>10 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 600M</td>
</tr>
<tr>
<td><strong>Regular</strong></td>
<td>6 CPU cores are allocated to tunnel processes. Maximum tunnel throughput: 400M</td>
</tr>
<tr>
<td><strong>Base</strong></td>
<td>2 CPU core are allocated to tunnel processes. Maximum tunnel throughput: 200M</td>
</tr>
<tr>
<td>* Local tunnel server address</td>
<td>The IP address and port number of the tunnel server. Default port: 1194</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Polycom recommends that you use the default port number 1194, but you can use any value from 1190-1199 or 65380-65389.</td>
</tr>
<tr>
<td>* Remote tunnel client address</td>
<td>The IP address and port number of the tunnel client. Default port: 1194</td>
</tr>
<tr>
<td>* Internal signal and media IP of tunnel client</td>
<td>The IP address of the network interface that the tunnel client uses for internal signaling and media communication with the RealPresence DMA system.</td>
</tr>
</tbody>
</table>
### Enable Tunnel
The tunnel feature is enabled if you have configured the tunnel server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Select <strong>Client</strong> to enable the system to operate as the tunnel client.</td>
</tr>
<tr>
<td>Client</td>
<td></td>
</tr>
<tr>
<td>Encrypted tunnel</td>
<td>When selected, tunnel communications are encrypted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td><em>This setting must be the same on both the tunnel server and tunnel client.</em></td>
</tr>
<tr>
<td>Performance profile</td>
<td>If tunnel encryption is enabled, select a performance profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td><em>The profiles on the tunnel server and client must match.</em></td>
</tr>
<tr>
<td></td>
<td><strong>Premium</strong>: 10 CPU cores are allocated to tunnel processes.</td>
</tr>
<tr>
<td></td>
<td>Maximum tunnel throughput: 600M</td>
</tr>
<tr>
<td></td>
<td><strong>Regular</strong>: 6 CPU cores are allocated to tunnel processes.</td>
</tr>
<tr>
<td></td>
<td>Maximum tunnel throughput: 400M</td>
</tr>
<tr>
<td></td>
<td><strong>Base</strong>: 2 CPU cores are allocated to tunnel processes.</td>
</tr>
<tr>
<td></td>
<td>Maximum tunnel throughput: 200M</td>
</tr>
<tr>
<td>* Local tunnel client address</td>
<td>The IP address and port number of the tunnel client. Default port: 1194</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Polycom recommends that you use the default port number 1194, but you can use any value from 1190-1199 or 65380-65389.</td>
</tr>
<tr>
<td>* Remote tunnel server address</td>
<td>The IP address and port number of the tunnel server. Default port: 1194</td>
</tr>
<tr>
<td>* Internal signal and media IP</td>
<td>The IP address of the network interface that the tunnel client uses for internal signaling and media communication with the RealPresence DMA system.</td>
</tr>
</tbody>
</table>
3 Click Update.

The system restarts.

The 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 Administrator’s Guide*.

You should configure certificates before federating your RealPresence Access Director system with another enterprise.

**Configure the RealPresence Resource Manager System**

In a 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.

To enable endpoint provisioning, see the following sections of this guide:

- “Add a Site for the RealPresence Access Director System” on page 18
- “Add a Provisioning User Account for Endpoints” on page 21

For complete instructions on configuring the RealPresence Resource Manager system, see the *Polycom RealPresence Resource Manager System Operations Guide for your version* of the RealPresence Resource Manager system.

**Configure the Polycom RealPresence DMA System**

See “Configure the Polycom RealPresence DMA System” on page 38.
Configure Additional Polycom Components

Refer to the following sections to configure additional Polycom components.

- “Configure Polycom Endpoint Systems” on page 26
- “Configure the Polycom RealPresence Collaboration Server” on page 27
- “Configure the Polycom RSS™ System” on page 27
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 Chapter 2, “Deploying the RealPresence Access Director System in a Corporate DMZ Environment” on page 11.

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
- 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, perform the following deployment tasks:

- Create additional DNS SRV records on the external DNS server
- Configure the RealPresence Access Director systems to support federated SIP calls
• 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” on page 12 describes the basic DNS setup required for this solution. Federating sites requires additional DNS configuration as described here.

• 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 (the DNS server configured on the Network Setting page of the RealPresence Access Director system) 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 an SRV record as follows.

_sips._tcp.example.com. IN SRV 0 0 5080 rpad.example.com.

Task 2 Configure the RealPresence Access Director systems to support federated SIP calls

To configure the federated sites’ RealPresence Access Director systems to support SIP calls

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

Complete this process on the RealPresence Access Director systems for the two sites being federated.

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.
   - 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 certificate is in the Trusted Store.

Task 3 Configure the Polycom RealPresence DMA systems to support federated SIP calls

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.

Complete this process on the RealPresence Access Director systems for the two sites being federated.

2 On the External SIP Peer tab, enter the internal signaling IP address of the RealPresence Access Director system as the Next hop address.

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.

10 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 federated (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 federated divisions or enterprises, perform the following deployment tasks:

- Configure the RealPresence Access Director systems to support federated H.323 calls
- Configure the Polycom RealPresence DMA Systems to support federated H.323 calls

Task 1

Configure the RealPresence Access Director systems to support federated H.323 calls

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


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.

Complete this process on the RealPresence Access Director systems for both of the enterprises being federated.
» 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.

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**

To configure the federated 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.

Complete this process on the RealPresence Access Director systems for both of the enterprises being federated.

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.
This chapter describes how to configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises.

In this deployment solution, one of the federated sites has a RealPresence Access Director. 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 Chapter 2, “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 enterprise 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 either uses an embedded or Polycom CMA system v6.2 gatekeeper.

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

• “Create an additional DNS A record on the external DNS server” on page 48
• “Create additional DNS SRV records on the external DNS server” on page 48
“Configure the RealPresence Access Director systems to support federated H.323 calls” on page 49

“Configure the Polycom RealPresence DMA System to support federated calls” on page 50

“Configure the CMA system to support federated H.323 calls” on page 50

“Configure the VBP-5300E system to support federated H.323 calls” on page 50.

Task 1

Create an additional DNS A record on the external DNS server

“Configure the DNS Service” on page 12 describes the basic DNS setup required for the RealPresence Access Director system in this solution. Federation requires additional DNS configuration as described here.

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 `vbp_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 federated H.323 calls

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

1  See the Polycom RealPresence Access Director Administrator’s 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.
   - CIDR should only include the subnet of the internal gatekeeper.

The CIDR is used by the RealPresence Access Director system to determine if the origin of a call is the internal network or external network. The value of CIDR depends on the local RealPresence DMA system mode (Routed or Direct).
   • If the local RealPresence DMA is configured in Routed mode, the CIDR should only include the subnet of the DMA system.
   • If the local RealPresence DMA system is configured in Direct mode, then the CIDR should include the subnet of the DMA system and local enterprise endpoints.

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 box as required

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 calls

To configure the federated enterprises’ RealPresence DMA system to support federated calls

1. See the *Polycom RealPresence DMA System Operations Guide* for detailed information about adding 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 v6.2 is the gatekeeper for the federated enterprise using the VBP-E access controller, perform this task. Otherwise, skip to “Task 7 (Conditional)” on page 51.

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

1. See the *Polycom CMA System Operations Guide* for detailed information about adding 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)” on page 51.
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.

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. Otherwise, skip to

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

To support calls from federated divisions or enterprises when an Acme Packet® Net-Net Enterprise Session Director (ESD) system is in the environment, perform the following configuration.

It is assumed here that the Acme Packet Net-Net ESD system is already installed and configured for standard use.

To configure the Acme Packet Net-Net ESD for federation

1  See the Acme Packet documentation at https://support.acmepacket.com/documentation.asp. Then add two realms (configure terminal; media-manager; realm-config). Configure the following mandatory parameters:

   identifier = B2B-Access
   description = For External Connection(Optional)
   network-interfaces = s0p0:0
identifier = B2B-Core
description = For Internal Connection(Optional)
network-interfaces = 1p0:0

2 Add two SIP interfaces (configure terminal; session-router; sip-interface). Configure the following parameters:

state enabled
realm-id B2B-Access
sip-port
  address 192.168.203.2 ACME Server External IP
  port 5061 ACME External Listening Port
  transport-protocol TLS ACME External Listening Transport
  tls-profile TLS-profile
  allow-anonymous all

state enabled
realm-id B2B-Core
sip-port
  address 192.168.204.2 ACME Server Internal IP
  port 5060
  transport-protocol UDP
  tls-profile
  allow-anonymous all

3 Add two steering pools (configure terminal; media-manager; steering-pool). Configure the following parameters:

ip-address 192.168.203.2 ACME Server External IP
start-port 60000
end-port 61999
realm-id B2B-Access

ip-address 192.168.204.2 ACME Server Internal IP
start-port 62000
end-port 63999
realm-id B2B-Core

4 Add two local policies (configure terminal; session-router; local-policy). Configure the following parameters:

local-policy
  from-address *
  to-address *
  source-realm B2B-Access
  state enabled
  policy-attribute
    next-hop 192.168.12.4-----DMA IP
    realm B2B-Core
Federation in a SIP Environment with Acme Packet

Federation Between RealPresence Access Director and Other

```
local-policy
from-address *
to-address *
source-realm B2B-Core
state enabled
policy-attribute
    next-hop 10.220.211.112----Another Enterprise IP
    realm B2B-Access
```

5 Save the configuration.
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.
The tables in this chapter define the required ports to configure for the RealPresence Access Director system.

- **Management Ports** on page 58
- **H.323 and WAN Ports** on page 61
- **H.323 and LAN Ports** on page 64
- **SIP and WAN Ports** on page 67
- **SIP and LAN Ports** on page 69
- **Tunnel Communication Ports** on page 72
- **Comparison of Tunnel Deployment and Standard Deployment Ports** on page 73

You can configure port range settings to decrease the number of dynamic ports that need to be open on your enterprise’s inside or outside firewall. A port range for a specific service indicates the number of ports that must be available to accommodate the number of calls for which your system is licensed.

After you have activated the license for your system, the RealPresence Access Director system automatically calculates the port ranges for your license. You can change port ranges as needed. See the *Polycom RealPresence Access Director System Administrator’s Guide*.

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

In the tables that follow, port ranges are indicated by a number in parentheses, followed by the port range values, as shown in this example:

(2)
13001-15000

Where (2) indicates SIP dynamic source ports and **13001-15000** is the range of port numbers.
Use the table below as a key for port range settings.

<table>
<thead>
<tr>
<th>Type of Ports</th>
<th>Transport</th>
<th>Associated Number in Port Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323 dynamic ports</td>
<td>TCP</td>
<td>(1)</td>
</tr>
<tr>
<td>SIP dynamic source ports</td>
<td>TCP</td>
<td>(2)</td>
</tr>
<tr>
<td>Access proxy dynamic source ports</td>
<td>TCP</td>
<td>(3)</td>
</tr>
<tr>
<td>External media ports</td>
<td>UDP</td>
<td>(4)</td>
</tr>
<tr>
<td>Internal media ports</td>
<td>UDP</td>
<td>(5)</td>
</tr>
</tbody>
</table>

**Management Ports**

The following tables describe the management ports on which the RealPresence Access Director system (RPAD) can listen.

For greater security, Polycom recommends that you disable SSH and Web access connectivity from the WAN, and enable SSH and Web access connectivity from the LAN. If you require the ability to manage the RealPresence Access Director system from the WAN, refer to the following tables for specific requirements.

**From the WAN to 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 the host managing the RPAD system via HTTPS</td>
<td>Any</td>
<td>TCP</td>
<td>* The RPAD system public management IP address</td>
<td>8443</td>
<td>HTTPS Web connectivity from the WAN client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host managing the RPAD system via SSH</td>
<td>Any</td>
<td>TCP</td>
<td>The RPAD system public management IP address</td>
<td>22</td>
<td>SSH connectivity from the WAN client to RPAD system</td>
</tr>
</tbody>
</table>

* The RealPresence Access Director system public management IP address refers to the public IP address mapped in the firewall located between the WAN and the RealPresence Access Director system.
### From the LAN to 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 the host managing the RPAD system via HTTPS</td>
<td>Any</td>
<td>TCP</td>
<td>* The RPAD system public management IP address</td>
<td>8443</td>
<td>HTTPS Web connectivity from internal client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host managing the RPAD system via SSH</td>
<td>Any</td>
<td>TCP</td>
<td>The RPAD system public management IP address</td>
<td>22</td>
<td>SSH connectivity from internal client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host sending an SNMP request to the RPAD system</td>
<td>Any</td>
<td><strong>UDP or TCP</strong></td>
<td>* The RPAD system public management IP address</td>
<td><strong>161</strong></td>
<td>SNMP connection from internal server to the RPAD system</td>
</tr>
</tbody>
</table>

* The RealPresence Access Director system public management IP address refers to the public IP address mapped in the firewall located between the WAN and the RealPresence Access Director system.

** The 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’s Guide for details.

### From the RealPresence Access Director System to the WAN

<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 management IP address</td>
<td>123</td>
<td>UDP</td>
<td>IP address of external NTP, if in use</td>
<td>123</td>
<td>NTP service from the RPAD system to the public NTP server</td>
</tr>
<tr>
<td>RPAD management IP address</td>
<td>30001 - 60000</td>
<td>TCP</td>
<td>IP address of external OCSP responder, if in use</td>
<td>8080</td>
<td>TCP connectivity from the RPAD system to the public OCSP responder</td>
</tr>
</tbody>
</table>
## From the RealPresence Access Director System to the LAN

<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 management IP address</td>
<td>30001 - 60000</td>
<td>UDP</td>
<td>IP address of external DNS, if in use</td>
<td>53</td>
<td>DNS service from the RPAD system to the internal DNS server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD management IP address</td>
<td>30001 - 60000</td>
<td>TCP</td>
<td>IP address of internal OCSP responder, if in use</td>
<td>8080</td>
<td>TCP connectivity from the RPAD system to the internal OCSP responder</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD management IP address</td>
<td>30001 - 60000</td>
<td>TCP</td>
<td>IP address of the internal Microsoft Active Directory LDAP server</td>
<td>389</td>
<td>RPAD system integration with Microsoft Active Directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD management IP address</td>
<td>30001 - 60000</td>
<td>* UDP or TCP</td>
<td>IP address of internal syslog server, if in use</td>
<td></td>
<td>Syslog service from the RPAD system to the internal syslog server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD management IP address</td>
<td>30001 - 60000</td>
<td>** UDP or TCP</td>
<td>IP address of internal SNMP server, if in use</td>
<td>**162</td>
<td>SNMP connectivity from the internal server to the RPAD system</td>
</tr>
</tbody>
</table>

* 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's Guide*.  
** The 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's Guide* for details.
H.323 and WAN Ports

The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s public IP address and the WAN for H.323 support.

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.

From the WAN to 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 H.323 devices</td>
<td>1719</td>
<td>UDP</td>
<td>* RPAD public signaling IP address</td>
<td>** 1719</td>
<td>Inbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>IP address of external H.323 devices</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>*** 1720</td>
<td>H.225 TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external H.323 devices</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>H.245 TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external H.323 devices</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>**** RPAD public media IP address</td>
<td>(4) (20002 - 30001)</td>
<td>Inbound RTP traffic transport from the WAN to the RPAD system</td>
</tr>
</tbody>
</table>

* The RealPresence Access Director system public signaling IP address refers to the public IP address for signaling mapped in the firewall located between the WAN and the RealPresence Access Director system.

** 1719 is the port used by remote H.323 endpoints to request registration with the RealPresence Access Director system.

*** 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.

**** The RealPresence Access Director system public media IP address refers to the public IP address for media mapped in the firewall located between the WAN and the RealPresence Access Director system.
### From the RealPresence Access Director System to the WAN

<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>(1)</td>
<td>TCP</td>
<td>IP address of external H.323 devices</td>
<td>* 1720</td>
<td>Outbound H.225 TCP connectivity for non-H.460 call scenarios</td>
</tr>
<tr>
<td></td>
<td>(10001 - 13000)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>(1)</td>
<td>TCP</td>
<td>IP address of external H.323 devices</td>
<td>&gt;1023</td>
<td>Outbound H.245 TCP connectivity for non-H.460 call scenarios</td>
</tr>
<tr>
<td></td>
<td>(10001 - 13000)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 1720 is the default H.225 TCP destination 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.

### From the WAN to the RealPresence Access Director System: H.323 B2B Calls

If you use the RealPresence Access Director system for H.323 enterprise-to-enterprise calls, the ports listed in the tables below are required in addition to those listed in the preceding table.

<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>Public signaling IP address of RPAD or VBP-E in the other enterprise</td>
<td>* 1719</td>
<td>UDP</td>
<td>RPAD public signaling IP address</td>
<td>** 1720</td>
<td>Inbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public signaling IP address of RPAD or VBP-E in the other enterprise</td>
<td>*** (I)</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>** 1720</td>
<td>Inbound H.225 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td>(10001 - 13000)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(RPAD - RPAD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(14085 - 15084)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(VBP-E - RPAD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public signaling IP address of RPAD or VBP-E in the other enterprise</td>
<td>(I)</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>(1)</td>
<td>Inbound H.245 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td>(10001 - 13000)</td>
<td></td>
<td></td>
<td>(10001 - 13000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(RPAD - RPAD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(14085 - 15084)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(VBP-E - RPAD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### H.323 and WAN 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>Public media IP address of RPAD or VBP-E in the other enterprise</td>
<td>(4) (20002 - 30001) (RPAD - RPAD) 16386 - 25386 (VBP-E 5300-E - RPAD)</td>
<td>UDP</td>
<td>RPAD public media IP address</td>
<td>(4) (20002 - 30001)</td>
<td>Inbound RTP traffic transport from WAN to RPAD for B2B call scenarios</td>
</tr>
</tbody>
</table>

* SRC Port 10001-10300 (RPAD-RPAD) assumes that a different enterprise RealPresence Access Director system also has 100 licenses and the default port range settings.

** DST Port 1720 is the default H.225 ports on the local RealPresence Access Director system. If you change the ports on the local system, you must also changed them accordingly on the firewall.

*** SRC Port 10001 - 10300 (RPAD-RPAD) assumes another enterprise RealPresence Access Director system also has 100 licenses and the default port pool settings.

### From the RealPresence Access Director System to the WAN: H.323 B2B Calls

<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 RPAD or VBP-E in the other enterprise</td>
<td>** 1719</td>
<td>Outbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>* (1) (10001 - 13000)</td>
<td>TCP</td>
<td>Public signaling IP address of RPAD or VBP-E in the other enterprise</td>
<td>** 1720</td>
<td>Outbound H.225 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>RPAD external signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>TCP</td>
<td>Public signaling IP address of RPAD or VBP-E in the other enterprise</td>
<td>*** (1) (10001 - 13000) (RPAD - RPAD) 14085 - 15084 (RPAD - VBP-E)</td>
<td>Outbound H.245 TCP connectivity for B2B call scenarios</td>
</tr>
</tbody>
</table>
**H.323 and LAN Ports**

The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s internal IP address and the LAN for H.323 support.

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 re-writing of port or IP address information.

### From the RealPresence Access Director System to the LAN

<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</td>
<td>* 1719</td>
<td>UDP</td>
<td>IP address of LAN-based H.323 Gatekeeper</td>
<td>** 1720</td>
<td>H.225 UDP connectivity from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td>signaling IP address</td>
<td></td>
<td></td>
<td>(DMA system)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on the local RealPresence Access Director system. If you change the port in the RealPresence Access Director system, you must also change it accordingly on the firewall.

** DST Ports 1719 and 1720 are the default H.225 ports on the RealPresence Access Director system or VBP-E of the other enterprise, so these two ports must be the same as the RealPresence Access Director system or VBP-E of the other enterprise.

*** DST Port 10001 -10300 (RPAD-RPAD) assumes another enterprise RealPresence Access Director system also has 100 licenses and the default port pool settings.

**** DST Port 20002-21001 (RPAD-RPAD) assumes another enterprise RealPresence Access Director system also has 100 licenses and the default port pool settings.
H.323 and LAN Ports

From the LAN to 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 signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 Gatekeeper (DMA system)</td>
<td>** 1720</td>
<td>H.225 TCP connectivity from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>TCP</td>
<td>IP address of LAN-based H.323 Gatekeeper (DMA system)</td>
<td>** 36000 - 61000</td>
<td>H.245 TCP connectivity from RPAD to LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on the local RealPresence Access Director system. If you change the port in the RealPresence Access Director system, you must also change it accordingly on the firewall.
** DST ports 1719 and 1720 are the default H.225 ports on a RealPresence DMA system, so the port must be the same on the RealPresence Access Director system.
*** 36000-61000 is the H.245 port range on a RealPresence DMA system.
If you use the RealPresence Access Director system for H.323 enterprise-to-enterprise calls, the ports listed in the tables below are required in addition to those listed in the preceding tables.

<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 LAN-based H.323 gatekeeper (DMA system)</td>
<td><strong>36000 - 61000</strong></td>
<td>TCP</td>
<td>RPAD internal signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>H.245 TCP connectivity from the LAN-based H.323 gatekeeper (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of LAN-based H.323 endpoints or MCUs</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD internal media IP address</td>
<td>(5) (40002 - 50001)</td>
<td>Outbound RTP traffic from the LAN H.323 clients to the RPAD system</td>
</tr>
</tbody>
</table>

* 1719 is the default H.225 UDP port on a RealPresence DMA system, so this port must be the same on the RealPresence Access Director system.
** 36000-61000 is the H.245 port range on a RealPresence DMA system.

**From the RealPresence Access Director System to the LAN: H.323 B2B Calls**

If you use the RealPresence Access Director system for H.323 enterprise-to-enterprise calls, the ports listed in the tables below are required in addition to those listed in the preceding tables.

<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>* 1719</td>
<td>UDP</td>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>**1719</td>
<td>Inbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on the local RealPresence Access Director system. If you change it on the local system, you must also change it accordingly on the firewall.
** DST Port 1719 is the default H.225 UDP port on a RealPresence DMA system, so this port must be the same on the RealPresence Access Director system.
From the LAN to the RealPresence Access Director System: H.323 B2B Calls

<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 LAN-based H.323 gatekeeper (DMA system)</td>
<td>* 1719</td>
<td>UDP</td>
<td>RPAD internal signaling IP address</td>
<td>** 1719</td>
<td>Outbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>36000 - 61000</td>
<td>TCP</td>
<td>RPAD internal signaling IP address</td>
<td>** 1720</td>
<td>Outbound H.225 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>36000 - 61000</td>
<td>TCP</td>
<td>RPAD internal signaling IP address</td>
<td>(1) (10001 - 13000)</td>
<td>Outbound H.245 connectivity for B2B call scenarios</td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on a RealPresence DMA system, so this port must be the same on the RealPresence Access Director system.

** DST Ports 1719 and 1720 are the default H.225 ports on the local RealPresence Access Director system. If you change the ports on the local system, you must also change them accordingly on the firewall.

SIP and WAN Ports

The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s public IP address and the WAN for SIP support with access proxy.

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.
### From the WAN to 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 SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>389</td>
<td>LDAP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>443</td>
<td>HTTPS connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>*5060</td>
<td>SIP TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD public signaling IP address</td>
<td>*5060</td>
<td>SIP UDP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>*5061</td>
<td>SIP TLS connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP address</td>
<td>5222</td>
<td>XMPP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD public media IP address</td>
<td>(4) (20002 - 30001)</td>
<td>Inbound RTP traffic transport from the WAN to the RPAD system</td>
</tr>
</tbody>
</table>
From the RealPresence Access Director System to the WAN

<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</td>
<td>(2)</td>
<td>TCP</td>
<td>Public signaling IP address of the RPAD</td>
<td>&gt;1023</td>
<td>SIP TCP connectivity for SIP B2B call scenarios</td>
</tr>
<tr>
<td>address</td>
<td>(13001-15000)</td>
<td></td>
<td>system or other enterprise SIP server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPAD external signaling IP</td>
<td>* 5060</td>
<td>UDP</td>
<td>Any IP address of external SIP clients</td>
<td>&gt;1023</td>
<td>SIP UDP connectivity from the RPAD system to the</td>
</tr>
<tr>
<td>address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WAN SIP clients</td>
</tr>
</tbody>
</table>

* 5060 is the default SIP external listening port on the RealPresence Access Director system. If you change this external port or have other SIP external listening ports on the RealPresence Access Director system, these ports must be changed or added accordingly on the firewall.

SIP and LAN Ports

The following table describes the required ports for DMZ port-filtering policies between RealPresence Access Director’s internal IP address and the LAN for SIP support with access proxy.

If your firewall has an SIP function that enables it to intercept and alter SIP messaging (for example, SIP ALG), you must disable the service. Failure to disable the service may cause call failures due to rewriting of port or IP address information.

From the RealPresence Access Director System to the LAN

<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</td>
<td>(2)</td>
<td>TCP</td>
<td>IP address of the LAN-based SIP registrar</td>
<td>* 5060</td>
<td>SIP TCP (5060) and SIP TLS (5061) connectivity</td>
</tr>
<tr>
<td>address</td>
<td>(13001-15000)</td>
<td></td>
<td>(DMA system)</td>
<td>5061</td>
<td>from the RPAD system to the LAN-based SIP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>registrar (DMA system)</td>
</tr>
<tr>
<td>SRC IP</td>
<td>SRC Port</td>
<td>Protocol</td>
<td>DST IP</td>
<td>DST Port</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>** 5070</td>
<td>UDP</td>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>* 5060</td>
<td>SIP UDP connectivity from the RPAD system to the LAN-based SIP registrar (DMA system)</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>(3) (30001 - 60000)</td>
<td>TCP</td>
<td>IP address of the LAN-based provisioning server (RealPresence Resource Manager system)</td>
<td>443</td>
<td>HTTPS connectivity from the RPAD system to the LAN-based provisioning server</td>
</tr>
<tr>
<td>RPAD additional interface IP address</td>
<td>(3) (30001 - 60000)</td>
<td>TCP</td>
<td>*** IP address of the LAN-based MEA*** server</td>
<td>443</td>
<td>HTTPS connectivity from the RPAD system to the LAN-based MEA server</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>(3) (30001 - 60000)</td>
<td>TCP</td>
<td>IP address of the LAN-based LDAP server</td>
<td>389</td>
<td>LDAP connectivity from the RPAD system to the LAN-based LDAP server</td>
</tr>
<tr>
<td>RPAD internal signaling IP address</td>
<td>(3) (30001 - 60000)</td>
<td>TCP</td>
<td>IP address of the LAN-based XMPP server</td>
<td>5222</td>
<td>XMPP connectivity from the RPAD system to the LAN-based XMPP server</td>
</tr>
</tbody>
</table>

* 5060, 5061 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.

** 5070 is the default SIP internal port on the RealPresence Access Director system. If you change this internal port on the RealPresence Access Director system, this port must be changed accordingly on firewall.

*** Polycom® Meeting Experience Application (MEA) server
From the LAN to 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 the LAN-based SIP registrar (DMA system)</td>
<td>* 5060</td>
<td>UDP</td>
<td>RPAD internal signaling IP address</td>
<td>** 5070</td>
<td>SIP UDP connectivity 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>&gt;1023</td>
<td>TCP</td>
<td>RPAD internal signaling IP address</td>
<td>** 5070 - 5071</td>
<td>SIP TCP connectivity from the LAN-based SIP registrar (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of LAN SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD internal media IP address (5) (40002 - 50001)</td>
<td>(5)</td>
<td>Outbound RTP traffic from LAN SIP clients to the RPAD system</td>
</tr>
</tbody>
</table>

* 5060 is the default SIP listening ports on the RealPresence DMA system, so the RealPresence Access Director system ports must be the same as those on the RealPresence DMA system.
** 5070 and 5071 are the default SIP internal ports on the RealPresence Access Director system. If you change these internal ports on the RealPresence Access Director system, the ports must be changed accordingly on the firewall.
# Tunnel Communication Ports

**From the RealPresence Access Director System Tunnel Server (DMZ) to the Tunnel Client (LAN)**

<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 local tunnel IP address</td>
<td>* 1194</td>
<td>UDP</td>
<td>RPAD remote tunnel IP address</td>
<td>1194</td>
<td>Connectivity between the RPAD tunnel server and the RPAD tunnel client</td>
</tr>
</tbody>
</table>

* 1194 is the default port for the RealPresence Access Director system local tunnel server and tunnel client.

**From the RealPresence Access Director System Tunnel Client (LAN) to the Tunnel Server (DMZ)**

<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 local tunnel IP address</td>
<td>* 1194</td>
<td>UDP</td>
<td>RPAD remote tunnel IP address</td>
<td>1194</td>
<td>Connectivity between the RPAD tunnel client and the RPAD tunnel server</td>
</tr>
</tbody>
</table>

* 1194 is the default port for the RealPresence Access Director system local tunnel server and tunnel client.
Comparison of Tunnel Deployment and Standard Deployment Ports

From the WAN to the RealPresence Access Director System and the RealPresence Access Director System to the WAN.

<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 tunnel and standard deployments (see Management Ports, From the WAN to the RealPresence Access Director System on page 58)</td>
<td>• The port range is the same for tunnel and standard deployments (see Management Ports, From the RealPresence Access Director System to the WAN on page 59)</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 tunnel and standard deployments (see H.323 and WAN Ports, From the WAN to the RealPresence Access Director System on page 61)</td>
<td>• The port range is the same for tunnel and standard deployments (see H.323 and WAN Ports, From the RealPresence Access Director System to the WAN on page 62)</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 tunnel and standard deployments (see SIP and WAN Ports, From the WAN to the RealPresence Access Director System on page 68)</td>
<td>• The port range is the same for tunnel and standard deployments (see SIP and WAN Ports, From the RealPresence Access Director System to the WAN on page 69)</td>
</tr>
</tbody>
</table>

From the LAN to the RealPresence Access Director System and the RealPresence Access Director System to the LAN.

<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 tunnel and standard deployments (see Management Ports, From the LAN to the RealPresence Access Director System on page 59)</td>
<td>• The port range is the same for tunnel and standard deployments (see Management Ports, From the RealPresence Access Director System to the LAN on page 60)</td>
</tr>
<tr>
<td><strong>Tunnel Port</strong></td>
<td><strong>Tunnel Port</strong></td>
</tr>
<tr>
<td>• Default is 1194 (see From the RealPresence Access Director System Tunnel Server (DMZ) to the Tunnel Client (LAN) on page 72)</td>
<td>• Default is 1194 (see From the RealPresence Access Director System Tunnel Server (DMZ) to the Tunnel Client (LAN) on page 72)</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” on page 75
- “DMZ Deployment with One or More Network Interfaces” on page 76
- “Two-system Tunnel Deployment” on page 77

### 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 signaling, media, and management 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.
DMZ Deployment with One or More Network Interfaces

When a RealPresence Access Director system with one network interface card is deployed in the enterprise DMZ (between two physical firewalls), all traffic uses one network interface and IP address.

If the RealPresence Access Director system with at least two network interfaces is deployed in the enterprise DMZ, both signaling and media services can be assigned to different interfaces for internal and external traffic. The figure below shows deployment in the enterprise DMZ, between two physical firewalls.

The following table lists the recommended network interface settings for the different communication services, 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 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>
</tbody>
</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>
</tbody>
</table>
Two-system Tunnel Deployment

In a 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 two network interfaces is deployed behind the inside firewall and acts as the tunnel client.

The tunnel server can forward all traffic through one open port on the inside firewall. If necessary, based on the firewall policy, the tunnel client can also send all traffic through one open port on the inside firewall.
The figure below illustrates a two-system tunnel deployment.

## Tunnel Server Network Interface Configuration

The following tables list the recommended tunnel server and tunnel client network interface settings for the different communication services, including the tunnel itself.

On the tunnel server, the network interface assigned to tunnel communication is the IP address and port number of the remote tunnel client.

<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, management, external signaling, and external media</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>Tunnel communication and management</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External signaling, External media</td>
</tr>
<tr>
<td>3</td>
<td>eth0</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External signaling, External media</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>Tunnel communication</td>
</tr>
<tr>
<td>4</td>
<td>eth0</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>External signaling</td>
</tr>
<tr>
<td></td>
<td>eth2</td>
<td>External media</td>
</tr>
<tr>
<td></td>
<td>eth3</td>
<td>Tunnel communication</td>
</tr>
</tbody>
</table>
Tunnel Client Network Interface Configuration

On the tunnel client, the network interface assigned to tunnel communication is the IP address and port number of the remote tunnel server.

<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, management, internal signaling, and internal media</td>
</tr>
<tr>
<td>2</td>
<td>eth0</td>
<td>Tunnel communication and management</td>
</tr>
<tr>
<td></td>
<td>eth1</td>
<td>Internal signaling</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal media</td>
</tr>
</tbody>
</table>