Release Notes

Polycom® RealPresence® Access Director™, Version 3.0

Polycom is pleased to announce the version 3.0 release of the Polycom RealPresence Access Director system. These release notes describe the key details about this release.

Contents

- "What's New in the Polycom RealPresence Access Director System Version 3.0 Release" on page 1
- "About the Polycom RealPresence Access Director System" on page 6
- "Licensing" on page 8
- "Installation Information" on page 8
- "Products Tested with this Release" on page 9
- "Open Source Software" on page 10
- "Resolved Issues" on page 11
- "Known Issues" on page 12
- "Where to Get the Latest Information" on page 17

What's New in the Polycom RealPresence Access Director System Version 3.0 Release

This release of the RealPresence Access Director system offers the following features and other changes. Each of these features is discussed in more detail in the following sections.

- "Split Interfaces for SIP and H.323 Signaling Traffic" on page 2
- "Tunnel Deployment of Two RealPresence Access Director Systems" on page 2
- "H.460 Endpoint Support" on page 2
- "Default Destination Alias for H.323 Guest Users" on page 3
- "Access Control Lists" on page 3
- "Call History and Registration History" on page 4
- "Port Ranges" on page 5
- "TCP Reverse Proxy" on page 5

October 2013
3725-78700-002B1

- "Interoperability with Cisco VCS Expressway™" on page 5
- "Enhanced Security Features" on page 5

Split Interfaces for SIP and H.323 Signaling Traffic

The RealPresence Access Director system supports the use of separate network interfaces for both signaling (SIP and H.323) and media services.

With the capability to split signaling and media communications, you can assign separate network interfaces and IP addresses for external and internal traffic. Separating external and internal signaling and media services both strengthens enterprise network security and increases the available bandwidth for calls.

Tunnel Deployment of Two RealPresence Access Director Systems

Two RealPresence Access Director systems can be deployed to tunnel traffic to and from your inside enterprise network. One RealPresence Access Director system is deployed in the enterprise back-to-back DMZ between the inside and outside firewall and acts as the tunnel server. The other system is deployed behind the inside firewall and serves as a tunnel client.

With the tunneling feature deployed, the tunnel server can forward all traffic through one open port on the inside firewall, thereby reducing the number of firewall ports that must be opened. If necessary, the tunnel client can also send all traffic through one open port on the inside firewall.

This deployment option allows you to configure the tunnel, including optional encryption, based specifically on your enterprise's security and firewall policies.

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.

H.460 Endpoint Support

The RealPresence Access Director system supports calls to and from H.460-enabled endpoints. The H.460 standard allows secure traversal of H.323 signaling across network address translators (NATs) and firewalls. The RealPresence Access Director system enables videoconference participants with both H.460-enabled endpoints or non-H.460 endpoints to register to a Polycom® RealPresence® Distributed Media Application™ (DMA™) system (H.323 gatekeeper) and place and receive H.323 calls across firewalls and NATs.

Default Destination Alias for H.323 Guest Users

The default destination alias feature enables the RealPresence Access Director system to assign a default destination alias to incoming H.323 guest calls that do not specify a destination alias for a Virtual Meeting Room (VMR).

Typically, H.323 calls without a destination alias are disconnected. However, when you configure a default destination alias, the RealPresence Access Director system uses the alias to route H.323 guest calls to the RealPresence DMA system gatekeeper.

The system supports both E.164 and H.323_ID aliases.

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 and rule settings define whether the RealPresence Access Director system allows or denies a specific type of SIP or H.323 request from a public network. The use of Access Control Lists provides increased protection against external security threats.

The Access Control List features provide numerous options for defining access rules and are highly configurable. You can use any of the default Access Control List rules within the RealPresence Access Director system or add your own rules to create white lists, black lists, and other access controls. Additionally, multiple Access Control List rules can be applied on one port.

Updating SIP External Port Settings

In previous versions of the RealPresence Access Director system, you could specify to **Forbid Registration** for specific SIP external ports. The **Forbid Registration** option is not available in version 3.0 of the RealPresence Access Director system. If you configured any SIP external ports to forbid registrations, this setting will not be applied to any SIP external ports after you upgrade to this version of the RealPresence Access Director system. To forbid registration on SIP external ports, you must create an Access Control List rule to deny SIP registration for the ports you specify.

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

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

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

4. Click **Add** and select the following options:
   - **Attribute: request.method**
   - **Operator: = =**
   - **Value: REGISTER**
5. Click **OK** twice.
6. Go to **Configuration > Access Control List Settings**.
7. Click **Add** and select the following options:
   - **Service Name: SIP**
   - **IP**: The IP address of the network interface assigned to external signaling.
   - **Port**: The external SIP port that will deny SIP registrations.
8. Click **Add** and select the following options:
   - **Access Control List Name**: the rule you created to forbid SIP registration (e.g., ACL-Deny-SIP-REGISTER)
   - **Action: Deny**
9. Click **OK**.

   The setting displays in the **Rule Setting** list.
10. Click **OK** to apply the rule.
11. Apply the rule to all ports that had **Forbid Registration** enabled in previous versions of your RealPresence Access Director system.

Call History and Registration History

The call history and registration history features offered in this version of the RealPresence Access Director system enable you to view detailed records of SIP and H.323 calls and endpoint device registrations. The historical records include details for call events, call subscription events, and device registration events.

Each feature offers robust search options that provide complete flexibility in finding the call and registration records in which you're interested. You can specify search criteria such as date and time ranges, signaling type, dial string, IP address, and other search options.

Consistent use of these features improves auditing and troubleshooting capabilities for your RealPresence Access Director system.

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 external 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 modify these ranges as needed.

TCP Reverse Proxy

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

A TCP reverse proxy connection can be bound to any existing interface, as well as the signaling port.

Interoperability with Cisco VCS Expressway™

The RealPresence Access Director system supports SIP and H.323 enterprise-to-enterprise calls to and from Cisco VCS Expressway.

Cisco VCS Expressway currently does not support enterprise-to-enterprise calls when SIP authentication is enabled in the RealPresence DMA system connected to the RealPresence Access Director system. See "Known Issues" on page 12.

Enhanced Security Features

Version 3.0 of the RealPresence Access Director system offers the following security enhancements:

- Server-side authentication
- Server-side session management
- Robust SIP TLS cipher
- OS hardening
- For new installations, the new default password for the Web user interface is **`Polycom123.`**
  - When upgrading the system from version 2.1 or 2.1.1 to version 3.0, the default password is **`admin`**.

About the Polycom RealPresence Access Director System

With the RealPresence Access Director system, Polycom offers a software-based edge server to securely route communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. This allows for secure communication between remote users and offices, and among guest users and organizations outside of the client's enterprise.

The RealPresence Access Director system combines the remote user, guest user, and enterprise-to-enterprise calling scenarios with SIP and H.323 capabilities. Additionally, the RealPresence Access Director system supports employee, guest, and federated calls from both AVC and SVC endpoints.

The RealPresence Access Director system produces combined value when integrated with the following Polycom components and endpoints.

- Polycom® RealPresence® Resource Manager systems provide management, provisioning, directory, and presence services.
- Polycom® RealPresence® Distributed Media Application™ (DMA™) systems serve as a central call control platform for SIP, H.323, and bridge virtualization, and act as H.323 gatekeepers.
- Polycom® RealPresence® Collaboration Server® systems serve as high-scale bridges for SIP and H.323 calls and support content over video.
- Polycom® RealPresence® CloudAXIS™ Suite is a software extension of the Polycom® RealPresence® Platform for private and public cloud deployment that enables businesses to collaborate with other businesses or individuals, independent of application, system, or device.
- Polycom® RSS™ systems enable recording of video, audio, and content.
- Polycom® RealPresence® Desktop supports sharing of video, audio, and content without leaving your desk.
- Polycom® RealPresence® Mobile enables tablets and smartphones to connect to video and audio conferencing and to share content.
- Polycom® RealPresence® Content Sharing Suite enables videoconferencing between Polycom endpoints and Microsoft Lync clients.
- Polycom® RealPresence® Group Series 300/500 endpoints
- Polycom® HDX endpoints

Features

The RealPresence Access Director system offers the following key features:

SIP Back-to-Back User Agent (B2BUA)

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

H.323 Signaling Proxy

- H.323 guest users
- H.323 enterprise-to-enterprise neighbored calling
- H.460 endpoint support

Media Relay

- RTP and SRTP pass through

Access Proxy

- Management (HTTPS/TLS)
- Presence (XMPP/TLS)
- Directory (LDAP/TLS)
- TCP reverse proxy

Security

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

Performance

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

Endpoints (AVC and SVC)

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

Licensing

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

If you deploy two RealPresence Access Director systems in a tunnel configuration, each system requires a separate license.

At installation, all new RealPresence Access Director systems come with a trial period license for five concurrent calls, to be used within 30 days after you activate your system license.

Installation Information

Installation and licensing of new RealPresence Access Director systems is managed through Polycom Global Services. For more information, please contact your Polycom representative.

Only versions 2.1 and 2.1.1 of the RealPresence Access Director system can be upgraded to version 3.0.

Visit the Polycom support site (http://support.polycom.com) to verify that you have the latest software release and release information for the product.

For installation and deployment information, refer to the following documents:

- *Polycom RealPresenceAccess Director Getting Started Guide*
- *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*
- *Polycom RealPresence Access Director Administrator's Guide*

Products Tested with this Release

Polycom RealPresence Access Director systems are tested extensively with a wide range of products. The following list is not a complete inventory of compatible equipment, but indicates the products that have been tested for compatibility with this release.

Product	Version
NAT, Firewall, Session Border Controllers	
Polycom RealPresence Access Director	3.0
Polycom Video Border Proxy (VBP) 5300E	11.2.16
Acme Packet® Net-Net 3820	SCX6.3.0 MR-2 GA (Build 385)
Management Systems and Recorders	
Polycom RealPresence Resource Manager	7.1.1 8.0
Polycom RSS 4000	8.5
Polycom RealPresence Content Sharing Suite	1.1.0
Microsoft Active Directory	
Gatekeepers, Gateways, and MCUs	
Polycom RealPresence Collaboration Server 1500, 2000, and 4000	7.8 8.1
Polycom RealPresence Collaboration Server 800s, Virtual Edition	7.8 8.1
Polycom RealPresence Distributed Media Application (DMA) 7000	6.0.2

Product	Version
Endpoints	
Polycom HDX 7000, 8000, and 9000 series	3.1.0 3.1.2
Polycom RealPresence Mobile	2.3 3.0
Polycom RealPresence Desktop	2.3 3.0
Polycom RealPresence Group Series 300/500	4.1.0 4.1.1

Polycom recommends that you upgrade all of your Polycom systems with the latest software versions before contacting Polycom support. Any compatibility issues may already have been addressed by software updates. Go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html to find the Polycom Current Interoperability Matrix.

Open Source Software

The Polycom RealPresence Access Director system uses several open source software packages, including the CentOS operating system. The following table lists the open source software packages used in the RealPresence Access Director system, the applicable license for each, and the internet address where you can find the software.

Software File Name	Version	License type	Source
aspectjrt-1.7.1.jar	1.7.1	Eclipse Public License - v 1.0	http://eclipse.org/aspectj/
aspectjtools-1.7.1.jar	1.7.1	Eclipse Public License - v 1.0	http://eclipse.org/aspectj/
javassist-3.11.0.GA.jar	3.11.0.GA	Mozilla Public License v1.1	http://www.mozilla.org/MPL/MPL-1.1.html
javolution-5.5.1.jar	5.5.1	BSD License	http://javolution.org/LICENSE.txt
oval-1.82.jar	1.82	Eclipse Public License - v 1.0	http://oval.sourceforge.net/license.html
paranamer-2.5.2.jar	2.5.2	BSD License	http://paranamer.codehaus.org/
drools-compiler-5.5.0.Final.jar	5.5.0	A simplified ASL/BSD/MIT-esque license	http://www.jboss.org/drools
velocity-1.7.jar	1.7	Apache License	http://velocity.apache.org/

Software File Name	Version	License type	Source
netty-4.0.0-CR3.jar	4.0.0- CR3	Apache License 2.0	http://netty.io/
spring-security-acl-2.0.8.RELEASE.jar	2.0.8	Apache License 2.0	http://static.springsource.org/spring-security/site/index.html
spring-security-core-2.0.8.RELEASE.jar	2.0.8	Apache License 2.0	http://static.springsource.org/spring-security/site/index.html
spring-security-core-tiger-2.0.8.RELEASE.jar	2.0.8	Apache License 2.0	http://static.springsource.org/spring-security/site/index.html
spring-security-taglibs-2.0.8.RELEASE.jar	2.0.8	Apache License 2.0	http://static.springsource.org/spring-security/site/index.html
as3corelib	.93build	BSD License	http://code.google.com/p/as3corelib/
intel-accel	1.5	BSD License	http://www.openssl.org/source/license.html
prototype.js	1.7.1	MIT License (source code) and CC-BY-SA (documentation)	http://http://prototypejs.org/
guava-13.0.1.jar	13.0.1	Apache License 2.0	https://code.google.com/p/guava-libraries/
openvpn-2.3.0	2.3.0	GPL 2.0	https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage

Resolved Issues

The following table lists the resolved issues in the version 3.0 release of the RealPresence Access Director system.

Issue ID	Description
EDGE-41	The RealPresence Access Director system uses the same flow token to different endpoints in UDP REGISTER message, leading to failed performance test.
EDGE-601	A RealPresence CloudAXIS Suite Web client cannot receive any audio-video content during calls routed through the RealPresence Access Director system.

Known Issues

The following table lists known issues in the version 3.0 release of the RealPresence Access Director system.

Category	Issue ID	Description	Workaround
Browser	EDGE-212	Two Internet Explorer 9 users unable to edit network settings screen.	Internet Explorer 9 issue, no workaround at this time.
Certificates	EDGE-267	The CA certificate isn't displayed when a certificate chain is installed.	
User Interface	EDGE-344	Vladivostok time zone is not UTC+10:00.	Linux OS issue, no workaround at this time.
User Interface	EDGE-351	The lan-cfg.txt file cannot be seen with the USB Network Utility.	
User Interface	EDGE-358	Polycom's former logo appears during installation of the RealPresence Access Director system.	
Endpoints	EDGE-489	When remotely upgrading RealPresence Group Series 300/500 endpoints through the RealPresence Access Director system, the upgrades fail. The Group Series 300/500 endpoints use HTTP to upgrade. The RealPresence Access Director system is an access device and supports only HTTPS for security purposes. When Group Series 300/500 endpoints support HTTPS upgrades, this issue will be resolved.	

Category	Issue ID	Description	Workaround
Call History	EDGE-666	Call history does not display an ACK record for a call from a remote user to the enterprise.	
User Interface	EDGE-697	When logging out of the RealPresence Access Director system after successful integration with Microsoft Active Directory and logging back in, the password field on the Microsoft Active Directory page in the user interface is blank.	
User Interface	EDGE-710	After a tunnel server or tunnel client is enabled, the browser displays a blank page and does not provide instructions to log back into the user interface.	Open the user interface again and log into the system.
User Interface	EDGE-713	Call history incorrectly displays the name of HDX systems.	
H.323	EDGE-718	Some H.323 endpoints cannot register through the RealPresence Access Director system due to a duplicated alias error.	Before upgrading to version 3.0 of the RealPresence Access Director system, update the RealPresenceDMA system to version 6.0.2.

Category	Issue ID	Description	Workaround
User Interface	EDGE-729	If version 3.0 of the RealPresence Access Director system is installed and then rolled back to version 2.x or later, a 404 error message displays when reopening the version 2.x user interface.	After installing version 3.0 and rolling back to version 2.0 or later, close all instances of Internet Explorer. Then reopen Internet Explorer, delete temporary internet files and cookies, and relaunch the version 2.x user interface.
SIP and H.323	EDGE-738	Registration History incorrectly displays the name of an H.323 endpoint that uses Chinese characters for the H.323_id. The system does not transfer a SIP REGISTER message to the RealPresence DMA system and the call fails if the SIP endpoint alias contains Chinese characters.	
H.323	EDGE-740	H.323 calls between an endpoint at one site and an endpoint on a different site fail to connect if routed through two hops of the RealPresence Access Director system.	
H.323	EDGE-747	H.323 calls between two endpoints located behind the same VBP 5300E server fail to connect.	
H.323	EDGE-748	An event detail message is not parsed if the H.323 service is not running when the user views H.323 events.	Enable H.323 signaling before viewing H.323 event details.

Category	Issue ID	Description	Workaround
Cisco VCS Expressway	EDGE-749	Cisco VCS Expressway currently does not support SIP enterprise-to-enterprise calls when an endpoint in an enterprise using Cisco VCS Control plus VCS Expressway calls an endpoint in an enterprise using the RealPresence Access Director system and a RealPresence DMA system if SIP authentication is enabled in the DMA system.	
RealPresence Mobile	EDGE-769	If briefly disconnected from the Internet or a network, RealPresence Mobile is automatically provisioned again but fails to successfully register again with the RealPresence Access Director system.	Sign out of RealPresence Mobile and sign back in.
Tunnel Configuration	EDGE-770	Enabling the tunnel feature with encryption fails if the time settings on the tunnel server and tunnel client are different. Tunnel status for both systems displays as **Pending**.	Synchronize the time on both the tunnel server and the tunnel client to the same NTP time server, then enable the tunnel with encryption.

Category	Issue ID	Description	Workaround
Access Control Lists	EDGE-779	When copying an Access Control List rule and modifying the name and conditions, the system saves the copied rule but does not apply the revised conditions when the rule is used. The conditions from the original rule remain in effect.	After copying an Access Control List rule, rename the copy and click **OK** in the **Copy rule** window without revising the conditions. Then select the new copied rule, click **Edit**, and revise the conditions as needed. Click **OK** in the **Edit rule** window for the revised conditions to take effect.
Tunnel Configuration	EDGE-781	In a tunnel configuration, calls may fail to connect if the performance profile differs on the tunnel server and tunnel client.	In **Configuration** > **Tunnel Settings**, select the same **Performance Profile** when configuring both the tunnel server and tunnel client.
Security	EDGE-786	OpenSSH 6.1 and prior installations have an overly long LoginGraceTime and a lack of early connection release for MaxStartups settings. If an unauthenticated remote attacker bypasses the thresholds, a denial of service can occur on the targeted server.	

Category	Issue ID	Description	Workaround
Tunnel Configuration	EDGE-790	With the tunnel feature enabled, H.323 calls from a registered remote user to an enterprise user fail to connect if the gatekeeper (the RealPresence DMA system) has been identified by FQDN instead of IP address.	From the tunnel server, go to **Configuration > H.323 Settings**. In the **Gatekeeper (Next hop) address** field, enter the IP address of the RealPresence DMA system. Do not use the FQDN.
Tunnel Configuration	EDGE-799	If a previous version of the RealPresence Access Director system uses separate interfaces for external and internal media traffic, the traffic is incorrectly routed after upgrading to version 3.0 if tunnel configuration is enabled before configuring the network interface settings.	For version 2.1 systems that use separate interfaces for external and internal media traffic, do the following: **1** Upgrade to version 3.0. **2** In network settings on both servers (tunnel server and tunnel client), configure separate interfaces for external and internal signaling. **3** Enable the tunnel.

Where to Get the Latest Information

To view the latest Polycom RealPresence Access Director system product documentation, visit the Support page of the Polycom website at

http://support.polycom.com

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.

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