Release Notes

3.1 | January 2014 | 3725-78700-002C

Polycom® RealPresence® Access Director™ System, Virtual Edition

Polycom announces the release of the Polycom RealPresence Access Director system, Virtual Edition, version 3.1. This document provides the latest information about this release.

Contents

New Features in Version 3.1

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.

SIP Open B2B Calling

This version of the RealPresence Access Director system supports SIP open business-to-business (B2B) calling, enabling calls to and from external SIP endpoints that are not registered or are not members of a federated enterprise or division.

The RealPresence Access Director system routes SIP open B2B calls only if you specify a valid default contact port for each type of transport. When the RealPresence Access Director system receives a SIP request message on the default contact port from a SIP endpoint that is not registered or is not a member of a federated enterprise or division, the system routes the call to the appropriate destination.

If you are deploying a RealPresence Access Director system for the first time, the default contact ports have been pre-configured as follows:

- TCP/UDP: 5060
- TLS: 5061

If you are upgrading your system from version 3.0, you must manually configure the default contact port for SIP open B2B for each type of transport. For instructions, see *Configuring SIP Settings* in the *Polycom RealPresence Access Director Administrator's Guide*.

Depending on your deployment configuration, you may need to create one or more DNS NAPTR records on your external-facing DNS server. For more information, see RFC 3263.

HTTP Reverse Proxy Tunnel

In this version, you can configure an HTTP tunnel reverse proxy that provides firewall traversal for Polycom® RealPresence® CloudAXIS™ Suite clients making SIP guest calls to video conferences. Specifically, the HTTP tunnel reverse proxy allows external CloudAXIS Suite clients to accept meeting requests from internal enterprise users and join the meetings as SIP guest users via standard HTTP ports, or non-standard ports that you configure. An HTTP tunnel reverse proxy enables the RealPresence Access Director system to act as a Web proxy and provide a bidirectional SIP signaling and media relay connection for HTTP requests.

Enhanced Access Proxy Features

The access proxy feature in the RealPresence Access Director system provides reverse proxy services for external client endpoints. You can configure reverse proxies to enable firewall/NAT traversal for various types of connections. When access proxy receives a request from an external client, the RealPresence Access Director system accepts the request and sends a new request on behalf of the client to the appropriate application server.

In version 3.1, the access proxy functionality offers increased flexibility to create multiple reverse proxy configurations as needed. The enhancements to access proxy enable you to do the following:

- Assign separate external and internal IP addresses for access proxy if you configure more than one network interface in your network settings. You can assign the IP addresses of up to four network interfaces as external IP addresses for access proxy.
- Create access proxy configurations that listen on one external IP address and unique port mapping per target application server and proxy communication requests to the appropriate internal application server.

- Use the default RealPresence Access Director system proxies or add new proxy configurations for the following services:
  - **HTTPS_proxy**: HTTPS servers that provide management services (Polycom® RealPresence® Resource Manager system, Polycom® RealPresence® Content Sharing Suite), RealPresence CloudAXIS Suite services, and other HTTPS application servers
  - **LDAP_proxy**: LDAP servers that provide directory services
  - **XMPP_proxy**: XMPP servers that provide message, presence, or other XMPP services
  - **PassThrough_proxy**: Web or other application servers not supported by the other access proxy protocols. Passthrough reverse proxy is used primarily for backwards compatibility with the TCP reverse proxy feature.
- Add an HTTP tunnel proxy. This type of proxy provides firewall traversal specifically for Polycom® RealPresence® CloudAXIS™ Suite clients making SIP guest calls to local network video conferences. See HTTP Reverse Proxy Tunnel on page 2 for further information.

Default Network Settings and Proxy Configurations for Access Proxy

The default network settings and access proxy configurations for version 3.1 differ based on whether you are installing the RealPresence Access Director system for the first time or upgrading an existing system.

New Installations

After a new installation, your system has the network and access proxy settings described below. Log into the RealPresence Access Director system user interface to view the settings.

Settings	Location	Value
Network Interface		
External access proxy IP address	Admin > Network Settings > Service network setting > Access Proxy Settings > External Access Proxy IP	IP address of eth0 network interface
Internal access proxy IP address	Admin > Network Settings > Service network setting > Access Proxy Settings > Internal Access Proxy IP	IP address of eth0 network interface
Default Access Proxy Configurations		
HTTPS_proxy	Configuration > Access Proxy Settings	External IP address: eth0 IP address External listening port: 443 You must configure additional settings, including next hops as needed.

Settings	Location	Value
XMPP_proxy	Configuration > Access Proxy Settings	External IPaddress: eth0 IP address External listening port: 5222 You must configure additional settings as needed.
LDAP_proxy	Configuration > Access Proxy Settings	External IPaddress: eth0 IP address External listening port: 389 You must configure additional settings as needed.

Upgrades

When you upgrade from version 3.0 of the RealPresence Access Director system to version 3.1, most of the access proxy settings you configured in version 3.0 are retained in version 3.1. The table below describes the network and access proxy settings and values for version 3.0 and any changes to these configuration details that occur after upgrading to version 3.1.

Version 3.0 Setting	Version 3.0 Value	Version 3.1 Setting	Version 3.1 Value	Version 3.1 Location
Network Interfaces				
External Signaling IP	IP address of the network interface you assigned as the External Signaling IP	External access proxy IP address	IP address of the network interface you assigned as the External Signaling IP in version 3.0	Admin > Network Settings > Service network setting > Access Proxy Settings > External Access Proxy IP
Internal Signaling IP	IP address of the network interface you assigned as the Internal Signaling IP	Internal access proxy IP address	IP address of the network interface you assigned as the Internal Signaling IP in version 3.0	Admin > Network Settings > Service network setting > Access Proxy Settings > Internal Access Proxy IP

Version 3.0 Setting	Version 3.0 Value	Version 3.1 Setting	Version 3.1 Value	Version 3.1 Location
Non-signaling IP	If you configured a TCP reverse proxy in version 3.0, the IP address of the network interface you assigned to TCP if different from the External Signaling IP or Internal Signaling IP	External access proxy IP address	IP address of the network interface you assigned to TCP reverse proxy in version 3.0	Admin > Network Settings > Service network setting > Access Proxy Settings > External Access Proxy IP
Default Access Proxy Configurations				
HTTPS	The settings you configured in version 3.0	HTTPS_proxy	The external and internal IP addresses of the default HTTPS_proxy, LDAP_proxy, and XMPP_proxy will be the IP addresses of the network interfaces you assigned to external and internal signaling in version 3.0. You can configure different IP addresses for the default proxies, and any new reverse proxies you add, after you select the external and internal access proxy IP addresses in the version 3.1 network settings.	Configuration > Access Proxy Settings > HTTPS_proxy
XMPP	The settings you configured in version 3.0	XMPP_proxy		Configuration > Access Proxy Settings > XMPP_proxy
LDAP	The settings you configured in version 3.0	LDAP_proxy		Configuration > Access Proxy Settings > LDAP_proxy

Version 3.0 Setting	Version 3.0 Value	Version 3.1 Setting	Version 3.1 Value	Version 3.1 Location
TCP	The TCP reverse proxy settings you configured in version 3.0 to enable connections to the Experience Portal (MEA) on an enterprise RealPresence CloudAXIS Suite server	PassThrough_proxy **Note** The PassThrough_proxy will not display on the main Access Proxy Settings page if you did not configure a TCP reverse proxy in version 3.0.	The external IP address of the PassThrough_proxy will be the IP address of the network interface you assigned to TCP reverse proxy in version 3.0. The internal IP address of the PassThrough_proxy will be the IP address of the network interface you assigned to internal signaling in version 3.0. **Note** In version 3.1, reverse proxy connections to a RealPresence CloudAXIS Suite Experience Portal (MEA) or Services Portal (WSP) should be configured as next hops within the default HTTPS_proxy, or a new HTTPS reverse proxy. For instructions, see the *Polycom RealPresence Access Director System Administrator's Guide*. After configuring an HTTPS proxy next hop with the information in PassThrough_proxy, you can delete the PassThrough_proxy.	Configuration > Access Proxy Settings > PassThrough_proxy

License Key for Two-box Tunnel Encryption

In version 3.1, the RealPresence Access Director system supports use of a license key to enable strong encryption of the tunnel between the tunnel server and tunnel client in a two-box tunnel deployment. If you purchase a license with a key that supports encryption, you can enable encryption of the two-box tunnel communication after you activate your license.

TLS Support for Microsoft Active Directory Server Integration

Different levels of security are supported for LDAP communication between the RealPresence Access Director system and the Microsoft Active Directory server. To increase the security of LDAP communication, version 3.1 offers the LDAP v3 extension StartTLS option to establish a TLS connection over the existing LDAP connection with the Microsoft Active Directory server. Polycom recommends use of the StartTLS option to provide the most secure LDAP communication.

Support for Polycom® CMA® Desktop Systems

The RealPresence Access Director system uses the H.460 standard to allow secure traversal of H.323 signaling across network address translators (NATs) and firewalls. Version 3.1 provides support to Polycom® CMA® Desktop system users with legacy H.323 endpoints. CMA Desktop system users can request provisioning from a RealPresence Resource Manager system, register to a Polycom® RealPresence® Distributed Media Application™ (DMA™) system (H.323 gatekeeper), and place and receive H.323 calls across firewalls and NATs.

New Features in Version 3.0

The version 3.0 release of the RealPresence Access Director system offered 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

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.

Two-box Tunnel Deployment of 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 two-box 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 two-box 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.

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 17.

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`.

Overview of the Polycom RealPresence Access Director System

The RealPresence Access Director system securely routes communication, management, and content traffic through firewalls without requiring special dialing methods or additional client hardware or software. Specifically, the RealPresence Access Director system supports SIP and H.323 calls from registered users, guests, and federated enterprises or divisions from both AVC and SVC endpoints. The system provides secure communication between remote users and offices, and among guest users and organizations outside of the client's enterprise network.

The RealPresence Access Director system provides the following key services:

SIP Back-to-Back User Agent

The RealPresence Access Director system serves as a SIP back-to-back user agent (B2BUA) and operates between both end points of a SIP video call session. When a SIP call takes place, the RealPresence Access Director system divides the communication channel into two call legs and mediates all SIP signaling between both ends of the call, from call establishment to termination.

The RealPresence Access Director system SIP B2BUA supports the following call scenarios:

- 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 remote users with H.460 endpoints
- H.323 guest users
- H.323 enterprise-to-enterprise neighbored calling

Media Relay

- RTP and SRTP pass through

Access Proxy

- Management, RealPresence CloudAXIS Suite, and other HTTPS application servers

- Presence (XMPP)
- Directory (LDAP)
- Passthrough reverse proxy to servers not supported by other access proxy protocols.
- HTTP tunnel (SIP signaling and media relay for SIP guest call HTTP requests from RealPresence CloudAXIS Suite clients)

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

Operating System

- CentOS 5.7 (2.6.18-274.el5)

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

Installation and Licensing

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

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

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

Each new RealPresence Access Director system comes with a trial period license for five concurrent calls, to be used within 60 days after your system was initially installed.

The system does not send notification when the 60-day trial period license is close to expiration. If you use the trial license before activating your purchased license, note the date when the trial period license expires to prevent any interruption to call services.

New Installations

For new installations, please contact your Polycom representative and refer to the *Polycom RealPresence Access Director System Getting Started Guide, Virtual Edition* for complete installation instructions. Then complete these tasks:

- Request an activation key code. See To request an activation key code on page 13.
- Activate your license. See To activate your license on page 13.

System Upgrades

RealPresence Access Director systems running version 3.0. of the software can be upgraded to version 3.1. If your system is not currently at version 3.0, you must perform interim upgrades before upgrading to version 3.1. The table below describes the interim upgrade scenarios:

Table: System Upgrade Scenarios

Starting RealPresence Access Director System Version	Upgrade to...
2.1	2.1.1
2.1.1	3.0
3.0	3.1

To request an activation key code

1. Open a web browser and go to http://support.polycom.com.
2. In the **Licensing & Product Registration** section, select **Activation/Upgrade**.
3. Select **All Other Polycom Products**.
4. Log in or **Register for An Account**.
5. Click **SITE & Single Activation/Upgrade**.
6. Accept the **EXPORT RESTRICTION** agreement.
7. In **Product Activation**, enter your VMware serial number (UUID) and click **Next**.
8. Click the **Upgrade Tab** to view the upgrade activation key codes available for your VMware serial number.
9. Record the activation key code for the upgrade and use it to activate your license after upgrading the software.

To upgrade the software

1. On your local system, create a directory to which to save the software upgrade file (bin file).
2. Download the software upgrade file to the local directory you created.
3. From the RealPresence Access Director system user interface, go to **Maintenance > Software Upgrade.**
4. From the **Actions** menu, click **Upload and Upgrade**.
5. Navigate to the upgrade package file, and click **Open**.

   After the upload is complete, the upgrading procedure begins automatically and the user interface closes.
6. After the upgrade is complete, open a new browser window and access the RealPresence Access Director system user interface.

   The End-user License Agreement displays.
7. Click **Accept** to advance to the log-in page.
8. Log into the user interface with these credentials:
   - User ID: **admin**
   - Password: **Polycom123**
9. Go to **Maintenance > Software Upgrade**.
10. Review the **System version** and **Operation History** to confirm the upgrade was successful.
11. Activate your license.

To activate your license

1. In the RealPresence Access Director system user interface, install the upgrade, then go to **Maintenance > License**.

2 Enter the **Activation key** for the license and click **Update**.

The system restarts.

Documentation

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

- *Polycom RealPresence Access Director System Getting Started Guide, Virtual Edition*
- *Deploying Polycom Unified Communications in RealPresence Access Director System Environments*
- *Polycom RealPresence Access Director System 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	3.1
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	8.0 8.1
Polycom RSS 4000	8.5
Polycom RealPresence Content Sharing Suite	1.2.0
Microsoft Active Directory	
Gatekeepers, Gateways, and MCUs	
Polycom RealPresence Collaboration Server 1500, 2000, and 4000	8.1 8.3
Polycom RealPresence Collaboration Server 800s, Virtual Edition	8.1
Polycom RealPresence Distributed Media Application (DMA) 7000	6.0.2 6.0.3

Product	Version
Endpoints	
Polycom HDX 7000, 8000, and 9000 series	3.1.0 3.1.2
Polycom RealPresence Mobile	3.0 3.1
Polycom RealPresence Desktop	3.0 3.1
Polycom RealPresence Group Series 300/500	4.1.2 4.1.3
Polycom Solution	
Polycom RealPresence CloudAXIS Suite	1.4.0

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.

Resolved Issues

The following table lists the resolved issues in the version 3.1 release of the RealPresence Access Director system.

Issue ID	Description
EDGE-212	Two Internet Explorer 9 users unable to edit network settings screen.
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.
EDGE-666	Call history does not display an ACK record for a call from a remote user to the enterprise.
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.
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.
EDGE-713	Call history incorrectly displays the name of HDX systems.

Issue ID	Description
EDGE-718	Some H.323 endpoints cannot register through the RealPresence Access Director system due to a duplicated alias error.
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.
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.
EDGE-747	H.323 calls between two endpoints located behind the same VBP 5300E server fail to connect.
EDGE-748	An event detail message is not parsed if the H.323 service is not running when the user views H.323 events.
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.
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.
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**.
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.
EDGE-781	In a tunnel configuration, calls may fail to connect if the performance profile differs on the tunnel server and tunnel client.
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.
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.

Known Issues

The following table lists the known issues of the RealPresence Access Director system, version 3.1, and of other products that affect use of the RealPresence Access Director system.

Category	Issue ID	Description	Workaround
Certificates	EDGE-915	When Online Certificate Status Protocol (OCSP) is enabled in the RealPresence Access Director system, OCSP does not check the server certificate unless mutual TLS for SIP signaling is configured between an endpoint and the RealPresence Access Director system.	
Certificates	EDGE-931	When creating a certificate signing request, up to 20 Subject Alternative Names (SANs) can be specified. If a SAN entry is deleted, leaving a blank line in the SAN list, the list of SANs does not update after clicking OK.	
User Interface	EDGE-937	In **Admin > SNMP Settings**, the **Local engine ID** field is blank.	
Polycom® CMA® Desktop **Note** This is a CMA Desktop issue and not a RealPresence Access Director system issue.	CMAD-10551	CMA Desktop systems located inside enterprise networks with certain restrictive firewall rules cannot view content shared by a remote CMA Desktop user when the content is routed through the RealPresence Access Director system.	
Polycom® RealPresence® Group Series 300/500 endpoints **Note** This is a Group Series issue and not a RealPresence Access Director system issue.	EDGE-489	When remotely upgrading a RealPresence Group Series 300/500 endpoint through the RealPresence Access Director system, the upgrade fails. The RealPresence Group Series 300/500 endpoints use the HTTP protocol to upgrade. For secure border management, the RealPresence Access Director system supports the HTTPS protocol. When RealPresence Group Series 300/500 endpoints support HTTPS upgrades, this issue will be resolved.	

Category	Issue ID	Description	Workaround
Cisco VCS Expressway **Note** This is a Cisco VCS Expressway issue and not a RealPresence Access Director system issue.	EDGE-749	A Cisco VCS Expressway call from an endpoint in an enterprise using Cisco VCS Control plus VCS Expressway to an endpoint in an enterprise using the RealPresence Access Director system and a RealPresence DMA system fails if SIP authentication is enabled in the DMA system. Cisco VCS Expressway currently does not support SIP enterprise-to-enterprise calls.	

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 America, Inc., 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 this product is available on the Polycom Support page for the RealPresence Access Director system.

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