RELEASE NOTES

Version 4.1 | April 2015 | 3725-78700-001E1

Polycom® RealPresence® Access Director™ System

Contents

What's New in Release 4.1

The RealPresence Access Director system version 4.1 includes the features and functionality of previous releases and releases and includes the following new features:

Basic Access Control Lists

To enhance the usability of Access Control Lists (ACLs), version 4.1 of the RealPresence Access Director system enables you to configure **Basic ACL Settings**. These settings provide simple-to-use control over inbound access to your video network through the RealPresence Access Director system. Basic ACL settings require you to enter minimal information about the allowed registrations and calls to your network. Based on your input, the RealPresence Access Director system then *automatically* creates the necessary ACL rules and settings on the appropriate ports to allow or deny access to your network.

In Basic ACL Settings, you can define the following registration policy and call policy settings:

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

Note that when you configure the Basic ACL Settings, you must specifically configure the sign-in, registration, or call requests to allow. If not specifically allowed, the system will deny requests.

Due to their ease of use, Polycom recommends the use of Basic ACL settings to control access to your video conferencing network. However, you can configure Advanced ACL settings to create specific customized ACL rules, conditions, variables, and settings, for your network.

Installation and Upgrade Considerations for Basic ACL Settings

In new installations of the RealPresence Access Director system version 4.1, the following basic Access Control List settings are enabled by default:

- Enable registration policy
- Allow registration from provisioned devices
- Enable call policy
- Allow call from registered devices

When you configure **Basic ACL Settings**, you must specify the registration or call requests to allow. The system will deny any requests that you do not allow within your settings. To ensure that the default basic ACL settings function as intended, be sure to configure your access proxy settings to enable endpoints to register and be provisioned. See the *Polycom RealPresence Access Director System Administrator Guide* for instructions.

When you upgrade to the RealPresence Access Director system version 4.1, none of the **Basic ACL Settings** are enabled. If you created any custom rules or settings in your previous version of the RealPresence Access Director system, these rules and settings will still be valid after you upgrade your system.

While not required, Polycom strongly recommends that you enable and configure **Basic ACL Settings** after you upgrade. When you do so, you must delete any settings that you previously configured for the system default rules or for any custom rules you created. Previous rule settings that allow or deny access when a rule is matched may conflict or be redundant with the **Basic ACL Settings** you configure in version 4.1 of the RealPresence Access Director system.

To delete rules settings from a previous version of the RealPresence Access Director system, complete the following steps:

1. In the web user interface, go to **Configuration > Advanced ACL Settings > Access Control List Rules** and view the rule type of each rule.
   - **Basic** rules are those that the system automatically creates when you enable and configure **Basic ACL Settings**.
   - **Advanced** rules are system default rules or custom rules that you created in the previous version of your RealPresence Access Director system.
2. Identify any custom rules and system default rules for which you previously configured settings.
3. Go to **Configuration > Advanced ACL Settings > Access Control List Settings**.
4. Select a rule setting that you configured in your previous version of the RealPresence Access Director system and click **Edit**.
   - Note that settings display based on the service type, IP address, and port number.
5. In **Advanced ACL rule settings**, select and **Delete** all rule settings.
6. Click **OK** and continue to delete all ACL rule settings you configured for your custom rules and for any of the system default rules.
7. *After* you delete the rule settings for advanced rules, test and verify that your **Basic ACL Settings** work correctly for your system.
8. Optional: After you verify that your **Basic ACL Settings** are configured as needed, you can delete the custom rules you previously created. Go to **Configuration > Advanced ACL Settings > Access Control List Rules** and delete the custom rules.

Enhanced Integration with the RealPresence Platform Director System

When you install version 4.1 of the RealPresence Access Director, Virtual Edition from the Polycom RealPresence Platform Director system, you can manually assign a static IP address to RealPresence Access Director, Virtual Edition or enable a DHCP server to obtain an IP address to use the first time your system starts. After you log into the RealPresence Access Director web user interface, you must assign a static IP address in network settings for each network interface. After you assign a static IP address, the DHCP service is disabled.

Note that each time your system starts up, it synchronizes the OS network IP addresses to the application database to ensure that all traversal services bind with the correct IP address.

Support for Higher Data Rate Transfer from RealPresence Content Sharing Suite Systems

The RealPresence Access Director system now supports higher data transfer rates for content sent from RealPresence Content Sharing Suite systems. In Access Proxy settings, you can configure the IP address of a RealPresence Content Sharing Suite system. When the RealPresence Access Director system receives BFCP over TCP content from this IP address, the system increases the data transfer rate for the content. This feature ensures successful content transfer from the RealPresence Content Sharing Suite system through the RealPresence Access Director system.

Integration with an F5 Load Balancer

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

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

F5 Load Balancer Limitations

Consider the following limitations if you deploy an F5 load balancer with your RealPresence Access Director systems:

- The security setting “Enable access proxy white list authentication for LDAP and XMPP access” does not function.
- The basic ACL setting “Allow registration from provisioned devices” does not function.

- Trusted B2B calls are treated as guest calls. The H.323 setting “Allow any incoming LRQ” must be enabled.

Other Changes in this Release

Default Security Setting for LDAP Requests

In the version 4.1 release of the RealPresence Access Director system, the security setting to **Enforce TLS for LDAP connection** is enabled by default. The RealPresence Access Director system will deny all LDAP connection requests sent from remote endpoints without TLS encryption.

Polycom strongly recommends that you disable this setting only if you need backward compatibility with Polycom RealPresence Group Series 300/500 endpoints that have not been upgraded to the most recent software version. Endpoints that have not been upgraded do not use an encrypted TLS connection when requesting LDAP services

You can find the **Enforce TLS for LDAP connection** option in the web user interface in **Admin > Security Settings** page.

Support of Google Chrome™ Browser

Version 4.1 of the RealPresence Access Director system supports use of the Google Chrome browser to access the web user interface.

Release History

This following table shows the release history of the RealPresence Access Director system:

Release History

Release	*API Release*	*System*	*Release Date*	*Features*
4.1	2.4.0	CentOS 6.4 Postgres 9.2 Java 7u21	December 2014	• Basic Access Control Lists • Enhanced Integration with the RealPresence Platform Director System • Support for Higher Data Rate Transfer from RealPresence Content Sharing Suite Systems • Integration with an F5 Load Balancer
4.0.1	2.4.0	CentOS 6.4 Postgres 9.2 Java 7u21	August 2014	• Resolved some known issues
4.0.0	2.4.0	CentOS 6.4 Postgres 9.2 Java 7u21	June 2014	• Upgrade operating system to CentOS 6.4 • Deploy and manage licenses using Polycom RealPresence Platform Director (Virtual Edition only) • Single interface and port for access proxy services and HTTP tunnel proxy • Firewall port mapping not required for two-system tunnel deployment • Support for BFCP/TCP content sharing through HTTP tunnel proxy • HTTP tunnel proxy auto-discovery • REST API (Virtual Edition) to support integration with the RealPresence Platform Director • License key to enable encryption of the tunnel in a two-system deployment • Other system enhancements
3.1.1	NA	CentOS 5.7 Postgres 9.1 Java 7u21	April 2014	• Support for Tandberg endpoints

Release	*API Release*	*System*	*Release Date*	*Features*
3.1.0	NA	CentOS 5.7 Postgres 9.1 Java 7u21	January 2014	• 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 • HTTP tunnel reverse proxy that provides firewall traversal for Polycom® integration with RealPresence Platform Director® CloudAXIS™ suite clients making SIP guest calls to video conferences • Increased flexibility of Access proxy services to support multiple reverse proxy configurations • License key to enable strong encryption of the tunnel between the tunnel server and tunnel client in a two-box tunnel deployment. • Support for the LDAP v3 extension StartTLS • Support for Polycom® CMA® Desktop Systems
3.0.0	NA	CentOS 5.7 Postgres 9.1 Java 7u21	August 2013	• Support for split interfaces for SIP and H.323 signaling traffic • Tunnel deployment of two RealPresence Access Director Systems • Support of H.460 endpoints • Support of default destination alias for H.323 guest users • Access control lists • Call history and registration history • Port ranges • TCP reverse proxy for Polycom® RealPresence® CloudAXIS™ suite clients • Interoperability with Cisco VCS Expressway™ • Enhanced security features
2.1.1	NA	CentOS 5.7 Postgres 9.1 Java 6u30	June 2013	• Resolved some known issues
2.1.0	NA	CentOS 5.7 Postgres 9.1 Java 6u30	March 2013	• Support for SNMP v2c and v3 for monitoring system status • Static route configuration • H.323 guest policy to limit destinations for inbound H.323 calls from the Internet • Support of both SVC and AVC endpoints for calls between federated enterprises

Release	*API Release*	*System*	*Release Date*	*Features*
2.0.4	NA	CentOS 5.7 Postgres 9.1 Java 6u30	January 2013	• Support for additional Polycom® RealPresence® products, including Content Sharing Suite, Collaboration Server 800s, Virtual Edition, and Group Series 300/500 • User interface updates • SIP and H.323 call disposition descriptions
2.0.3	NA	CentOS 5.7 Postgres 9.1 Java 6u30	December 2012	• SIP Back-to-Back User Agent (B2BUA) • H.323 signaling proxy for guest users and enterprise-to-enterprise federated calling • Media relay, including RTP and SRTP passthrough and SVC support for SIP remote users • Access proxy for management, presence, and directory traffic • DMZ deployment • Support for managed endpoints (Polycom HDX systems, RealPresence Mobile, RealPresence Desktop)

Hardware Requirements

You need a computer running Microsoft® Windows® to install the RealPresence Access Director system and configure the initial settings. The computer requires a minimum display resolution of 1280x1024 (SXGA). A resolution of 1680x1050 (WSXGA+) is recommended.

Software Requirements

The following table describes the software requirements for the RealPresence Access Director system.

Software Requirements

Product	*Versions*
Browsers supported:	
Microsoft Internet Explorer®	8 or higher
Google Chrome™	NA
Java™	7
Adobe® Flash® Player	11 or higher

System Capabilities and Constraints

The RealPresence Access Director system is available as an Appliance Edition or Virtual Edition.

As of April 1, 2015, the RealPresence Access Director, Appliance Edition, is available on either a Polycom Rack Server 220 (R220) or a Polycom Rack Server 620 (R620).

Appliance Edition

When installed on a Polycom Rack Server 220 (R220), the RealPresence Access Director system supports the following maximum system capabilities:

Capability	*R220 Maximum*
Registrations	2000
Concurrent calls (one system)	200
Concurrent calls (two-systems in tunnel configuration)	150
HTTPS tunnel calls (Polycom® RealPresence® CloudAXIS™ Suite SIP only)	50
Throughput (Mbps)	700

Virtual Edition

The RealPresence Access Director, Virtual Edition, system software can be installed in a virtual data center environment.

Virtual Edition Host Server Hardware Profiles

For the RealPresence Access Director, Virtual Edition, the following table describes the minimum server requirements for each instance that you install.

Virtual Machine Host Server Hardware Profile

Component	*Minimum Profile*
CPU Limit	5000 MHz
CPU Reservation Limit	2000 MHz

Component	*Minimum Profile*
Memory Reservation	4 GB
Storage	64 GB
Number of concurrent calls (five calls per second)	70

The throughput capacity for the preceeding profile is 10 MB.

Interoperability Constraints

The following table lists known issues of other products that may cause interoperability issues with the RealPresence Access Director system.

Interoperability Issues

Product	*Description*
Cisco VCS Expressway	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.

Products Tested with this Release

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

Note: Update your system

Polycom recommends that you upgrade all of your Polycom systems with the latest software versions, as compatibility issues may already have been addressed by software updates. Go to PolycomService/support/us/support/service_policies.html to see the Current Polycom Interoperability Matrix.

Products Tested with this Release

Product	*Tested Versions*
NAT, Firewall, Session Border Controllers	
Polycom RealPresence Access Director	4.1
Polycom Video Border Proxy (VBP) 5300E	11.2.18
Acme Packet® Net-Net ESD 3820	6.3
Management Systems	
Polycom RealPresence Resource Manager	8.2, 8.3
Polycom RealPresence Content Sharing Suite	1.3., 1.4
Microsoft Active Directory	
Web Browser-Based Solutions	
Polycom RealPresence CloudAXIS Suite	1.6.x
Gatekeepers, Gateways, and MCUs	
Polycom RealPresence Collaboration Server (RMX) 1500, 2000, and 4000	8.4, 8.5
Polycom RealPresence Distributed Media Application (DMA) 7000	6.1.x, 6.2
Endpoints	
Polycom HDX 7000, 8000, and 9000 series	3.1.3, 3.1.4
Polycom RealPresence Mobile	3.2

Product	*Tested Versions*
Polycom RealPresence Desktop	3.2, 3.3
Polycom RealPresence Group Series 300/500	4.1.3, 4.2
Cisco C20 Codec	TC7.1.1
Cisco C40 Codec	TC7.1.1
Cisco EX60 Desktop System	TC7.1.1
Cisco EX90 Desktop System	TC7.1.1
Cisco 1700 MXP Desktop System	F9.3.1
RealPresence Platform Virtual Edition Infrastructure	
Polycom RealPresence Platform Director • VMware vCenter Server	1.7. 5.1, 5.5

Installation and Upgrade Notes

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

Polycom RealPresence Platform, Virtual Edition products such as the RealPresence Access Director system, Virtual Edition require the RealPresence Platform Director™ solution to install the software and manage licensing. The RealPresence Platform Director system provides the flexibility to deploy, license, and monitor the RealPresence Platform, Virtual Edition products using general purpose hardware in an organization's data center or in the cloud.

The RealPresence Platform Director system is available at no charge on Polycom's support website (http://support.polycom.com).

Note: Get the latest product information from Polycom Support

To confirm that you have the latest software release and product documentation, visit the Support page of the Polycom web site at http://support.polycom.com.

RealPresence Access Director systems running version 4.0.x of the software can be upgraded to version 4.1. If your system is not currently running version 4.0.x, you must perform intermediate upgrades before upgrading to version 4.1.

Polycom supports the following upgrade paths for the RealPresence Access Director system version 4.1. Read all relevant Release Notes before upgrading to an intermediate version.

Upgrade Paths

Current Version	*Intermediate Upgrade*	*Final Version*
Prior to version 2.1.x	2.1.x	*3.0*
3.0		3.1.x
3.1.x	4.0 **Note:** This version of the RealPresence Access Director System, Virtual Edition cannot be upgraded from version 3.1.x and instead requires a new installation and data migration.	4.0.1
4.0.x		4.1

You can upgrade both the Appliance Edition and Virtual Edition of the RealPresence Access Director system to version 4.1 from the **Maintenance > Software Upgrade** page of the system's web interface.

To upgrade to version 4.1 of the RealPresence Access Director system:

1. Create a backup of your current system and download it to your local computer.
2. Download the version 4.1 upgrade file (*.bin file) from the Polycom support site (http://support.polycom.com).
3. Follow the instructions in the *Polycom RealPresence Access Director System Administrator Guide* or the online help to upgrade the system to version 4.1.
4. After the upgrade is complete, clear the cache of your browser to ensure that the RealPresence Access Director web user interface displays all updated components.
5. From your browser, log into the system's web interface with the following credentials:
   - User ID: **admin**
   - Password: **Polycom12#$**
6. Go to **Maintenance > Software Upgrade**.
7. Review the System Version field and Operation History list to confirm the upgrade was successful.
8. If you are upgrading the RealPresence Access Director, Appliance Edition, request a new license activation key code for version 4.1, then activate your license in the web user interface.

Known Issues

The following table lists all known issues of the RealPresence Access Director system.

Known Issues

Category	*Issue No.*	*Found in Release*	*Description*	*Workaround*
Open SIP Calls	EDGE-1360	4.0.1	When a SIP endpoint makes an open SIP call through a RealPresence Access Director system to a second endpoint with a RealPresence Access Director system, the call connects. If the call lasts more than five minutes and the second (callee) endpoint hangs up, the first endpoint does not release the call.	
H.323 Call Quality	EDGE-1349	4.1.0	Video latency occurs in H.323 calls from an external Huawei H.460-enabled endpoint to an internal Polycom RealPresence Group Series endpoint.	
H.323 Call Quality	EDGE-1348	4.1.0	Video latency occurs in H.323 calls from an external Sony H.460-enabled endpoint to an internal Polycom RealPresence Group Series endpoint.	
H.323 Call Quality	EDGE-1332	4.1.0	Video latency occurs in H.323 calls from an external LifeSize H.460-enabled endpoint to an internal Polycom RealPresence Group Series endpoint.	
Access Proxy	EDGE-1385		After a system restart, the Access Proxy service may not function correctly, which causes CloudAXIS Suite calls to fail.	

Category	*Issue No.*	*Found in Release*	*Description*	*Workaround*
System Logs, Virtual Edition	EDGE-1389		In the Virtual Edition, the web user interface cannot be accessed if the log partition is full.	After initial installation, follow these steps to prevent the issue from occurring: • Go to **Admin > Log Settings**. • Change the **Retention period (days)** from 7 days (default) to 1–3 days. If the issue occurs before you configure the log retention period, contact Polycom Global Services.

Resolved Issues

The following table lists the issues resolved in version 4.1 of the RealPresence Access Director system.

Resolved Issues

Category	*Issue Number*	*Found in Release*	*Description*
Installation, Virtual Edition	EDGE-1309	4.0.1	The RealPresence Access Director, Virtual Edition, *.ova* file does not deploy.
SIP Settings	EDGE-1236	3.1.0	On the SIP Settings page, changes made to the internal port settings are not saved after updating.
SIP Registrations	EDGE-1217	4.0.0	The SIP module does not forward registration refresh messages from a port that has the Access Control List All_Matches rule applied with the rule setting configured as deny.
Certificates	EDGE-1210	4.0.0	Only a limited selection of special characters are allowed in the fields a Certificate Signing Request (CSR).
Upgrade	EDGE-1109	3.1.0	After an upgrade file has been uploaded, user must click *Complete* to close the status bar indicator. Without clicking *Complete*, the upload does not display in the Operation History table on the Software Upgrade page.
Certificates	EDGE-989	4.0.0	An open SIP TLS call fails from an endpoint in a network with a RealPresence Access Director system to an endpoint in a different network that also has a RealPresence Access Director system. The first RealPresence Access Director system reports an alert when there is no root CA for the second RealPresence Access Director system.
Time Settings	EDGE-344	2.0.0	Vladivostok time zone is not UTC+10:00.

Get Help

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

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

For more information on solution with this Polycom partner, see the partner site at *Polycom Global Strategic Partner Solutions*.

The Polycom Community

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

Copyright and Trademark Information

6001 America Center Drive

San Jose, CA 95002

USA

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the *End User License Agreement* for this product.

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.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided “as is” without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Visit the *Polycom Support Center* for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.