

Polycom® RealPresence® Access Director™ System

Contents

What's New in Release 4.2.5.....	2
Security Updates.....	3
Release History	3
Products Tested with this Release	7
System Capabilities and Constraints	9
Hardware Requirements	10
Software Requirements.....	10
Installation and Upgrade Notes.....	11
Resolved Issues.....	13
Known Issues.....	15
Get Help	17
Copyright and Trademark Information.....	18

What's New in Release 4.2.5

The Polycom® RealPresence® Access Director™ system version 4.2.5 includes the features and functionality of previous releases and provides the following enhancements:

- [Enhanced Security Settings](#)
- [Viewing Usage Data and Settings](#)

Enhanced Security Settings

This version of the RealPresence Access Director system offers enhanced security options. You can configure your system to allow or disallow the following security settings:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- DES/3DES Ciphers
- Weak RSA Ciphers

All settings are enabled by default for new installations and upgrades of the RealPresence Access Director system version 4.2.5. Note that if you disable any of the settings, you must ensure that all devices on your network that interact with the RealPresence Access Director system must also support disabling of the same security settings. For example, if you disable TLS 1.1, any device on your network that does not support TLS v1.2 or higher will not work with the RealPresence Access Director system version 4.2.5 if TLS is required for encryption.

Note that at least one TLS setting must be selected.

Viewing Usage Data and Settings

When you accept the End User License Agreement (EULA) for the RealPresence Access Director system, you can select the **Automatically send usage data** check box. This option enables your system to send various types of usage data to a Polycom collection point (customerusagedatacollection.polycom.com). As this data is used to continually improve the product, Polycom recommends that you keep the setting enabled. See the *Automatically Send Usage Data* section in the *Polycom® RealPresence® Access Director™ System Administrator Guide* for a description of the type of data your system sends.

To view if you selected the **Automatically send usage data** option:

- » Go to **Maintenance > License Server Settings** in the web user interface.

To see the data your RealPresence Access Director system sends to Polycom:

- 1 Go to **Diagnostics > System Log Files** in the web user interface.
- 2 Under **Actions**, click **Roll Logs**.
The system prompts you to download the log archive.
- 3 Click **OK** and save the log archive to your local machine.

4 After the download is complete, unpack the log archive.

The *analytics.json* file in the *var/log/polycom/rpp* directory contains the data that your RealPresence Access Director system sends to Polycom.



Note: If your local DNS server does not resolve *customerusagedatacollection.polycom.com*, the analytics service in the RealPresence Access Director system will query the Google DNS server (8.8.8.8) to resolve that DNS name.

Security Updates

This release includes the following security-related changes:

- *CVE-2016-0636: Upgraded JRE to address security vulnerability in Oracle Java SE 7u97, 8u73, and 8u74.*
- *CVE-2016-5195: Resolved Linux kernel security vulnerability.*
- *CVE-2015-4000: Resolved SSH configuration vulnerability.*
- *Fixed issue with missing session cookie in HttpOnly attribute.*
- *Removed JBoss JMX Console and Web Console unused code.*
- *Increased length of web session token to more than 50 characters.*
- *Discontinued use of insecure cipher suites.*

Please refer to the [Polycom Security Center](#) for information about known and resolved security vulnerabilities.

Release History

This following table lists the release history of the RealPresence Access Director system.

Release History

Release	System	Release Date	Features
4.2.5	CentOS 6.8 PostgreSQL 9.3.9 OpenJDK 1.7.0.131- 2.6.9.0.el6_8.x86_64	March 2017	<ul style="list-style-type: none"> • Security enhancements • Bug fixes
4.2.4	CentOS 6.8 PostgreSQL 9.3.6 OpenJDK 1.7.0.101- 2.6.6.4.el6_8.x86_64	November 2016	<ul style="list-style-type: none"> • Enhancements • Bug fixes

<i>Release</i>	<i>System</i>	<i>Release Date</i>	<i>Features</i>
4.2.3	CentOS 6.7 PostgreSQL 9.3.6 OpenJDK 1.7.0.79-2.5.5.1	March 2016	<ul style="list-style-type: none"> • Support for RealPresence Clariti solution • Support for disabling TLS v1.0 • Change to interpretation of VMR ranges • Support for VMware vSphere Platform version 6.0 • Resolved some known issues
4.2.2	CentOS 6.7 PostgreSQL 9.3.6 OpenJDK 1.7.0.79-2.5.5.1	December 2015	<ul style="list-style-type: none"> • Resolved some known issues
4.2.1.1	CentOS 6.7 PostgreSQL 9.3.6 OpenJDK 1.7.0.79-2.5.5.1	September 2015	<ul style="list-style-type: none"> • Resolved some known issues
4.2.1	CentOS 6.7 PostgreSQL 9.3.6 OpenJDK 1.7.0.79-2.5.5.1	August 2015	<ul style="list-style-type: none"> • Support for SHA-256 SSL certificates • Security updates • Resolved some known issues
4.2	CentOS 6.6 PostgreSQL 9.3.6 OpenJDK 1.7.0.79-2.5.5.1	June 2015	<ul style="list-style-type: none"> • High Availability deployment option • STUN and TURN service to support WebRTC video conferencing • Support for Hyper-V virtual environments • Operating system upgraded to CentOS 6.6 • Replaced Oracle JDK with OpenJDK
4.1	CentOS 6.4 Postgres 9.2 Java 7u21	December 2014	<ul style="list-style-type: none"> • 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	CentOS 6.4 Postgres 9.2 Java 7u21	August 2014	<ul style="list-style-type: none"> • Resolved some known issues

<i>Release</i>	<i>System</i>	<i>Release Date</i>	<i>Features</i>
4.0.0	CentOS 6.4 Postgres 9.2 Java 7u21	June 2014	<ul style="list-style-type: none"> • Operating system upgraded 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	CentOS 5.7 Postgres 9.1 Java 7u21	April 2014	<ul style="list-style-type: none"> • Support for Tandberg endpoints
3.1.0	CentOS 5.7 Postgres 9.1 Java 7u21	January 2014	<ul style="list-style-type: none"> • 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

<i>Release</i>	<i>System</i>	<i>Release Date</i>	<i>Features</i>
3.0.0	CentOS 5.7 Postgres 9.1 Java 7u21	August 2013	<ul style="list-style-type: none"> • 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	CentOS 5.7 Postgres 9.1 Java 6u30	June 2013	<ul style="list-style-type: none"> • Resolved some known issues
2.1.0	CentOS 5.7 Postgres 9.1 Java 6u30	March 2013	<ul style="list-style-type: none"> • 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
2.0.4	CentOS 5.7 Postgres 9.1 Java 6u30	January 2013	<ul style="list-style-type: none"> • 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	CentOS 5.7 Postgres 9.1 Java 6u30	December 2012	<ul style="list-style-type: none"> • 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)

Products Tested with this Release

RealPresence Access Director systems are tested extensively with a wide range of products. The list in this section is not a complete inventory of compatible systems. Rather, the list includes the products that have been tested for compatibility with this release.

Polycom supports mixed Hyper-V/VMware environments, but has not tested all configurations and combinations.



Note: Polycom recommends that you upgrade all of your Polycom systems with the latest software versions. 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 see the current Interoperability Matrix.

Products Tested with this Release

<i>Product</i>	<i>Tested Versions</i>
NAT, Firewall, Session Border Controllers	
Polycom RealPresence Access Director	4.2.5
Management Systems	
Polycom RealPresence Resource Manager	8.3, 9.0.1, 10.x
Microsoft Active Directory	Microsoft Windows Server 2012 R2
Web Browser-Based Solutions	
Polycom RealPresence Web Suite	2.1
Gatekeepers, Gateways, and MCUs	
Polycom RealPresence Distributed Media Application (DMA) 7000	6.3.2, 6.4.1
Polycom RealPresence Collaboration Server	8.6, 8.6.3, 8.7.1
Polycom RMX 1500/2000/4000 (MPMx)	8.5.x
Endpoints	
Polycom RealPresence Group Series 500/700; 310; 550	4.3.0, 5.1.0
Polycom HDX 7000	3.1.3, 3.1.4, 3.1.10
Polycom RealPresence Desktop	3.7
Polycom RealPresence Mobile	3.6

<i>Product</i>	<i>Tested Versions</i>
RealPresence Platform Virtual Edition Infrastructure	
Polycom RealPresence Platform Director (required for virtual edition customers as well as RealPresence Clariti customers)	3.0
Hypervisor Environments for Virtual Editions	
VMware vSphere Platform	5.5, 6.0
Microsoft Hyper-V	Microsoft Windows Server 2012 R2 with the Hyper-V role enabled

Interoperability Issues

The following table lists potential interoperability issues when using the RealPresence Access Director system, version 4.2.5.

Interoperability Constraints

<i>Product</i>	<i>Description</i>
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 RealPresence DMA system. Cisco VCS Expressway currently does not support SIP enterprise-to-enterprise calls.
Sony H.460-enabled endpoint	Video latency occurs in H.323 calls from an external Sony H.460-enabled endpoint to an internal Polycom RealPresence Group Series endpoint.
LifeSize H.460-enabled endpoint	Video latency occurs in H.323 calls from an external LifeSize H.460-enabled endpoint to an internal Polycom RealPresence Group Series endpoint.
Cisco PIX 515E firewall, version 7.1(2)	Rapid network outages may cause the Address Resolution Protocol (ARP) table in the firewall to have an incorrect MAC address for a RealPresence Access Director system configured for High Availability. This situation causes signaling for registrations and calls to that system to fail. Cisco no longer supports this firewall model.

System Capabilities and Constraints

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

The system software for the RealPresence Access Director, Appliance Edition, can be installed on the following Polycom servers:

- Polycom Rack Server 220 (R220)
- Polycom Rack Server 230 (R230)
- Polycom Rack Server 620 (R620)
- Polycom Rack Server 630 (R630)

Appliance Edition

When installed on a Polycom R630, R620, R230, or R220 server, the RealPresence Access Director system supports the maximum capabilities listed in the following table.

RealPresence Access Director Maximum Server Capabilities

Capability	R220	R230	R620	R630
Registrations	2000	2000	5000	5000
Concurrent calls	200	200	1000*	1000*
HTTPS tunnel calls (Polycom® RealPresence® Web Suite SIP guest calls only)	50	50	50	50
Throughput (Mbps)	700	700	700	700

* Maximum concurrent call numbers will depend on the overall deployment model, network quality, codecs used, total throughput of all calls, and available bandwidth.

Virtual Edition

The RealPresence Access Director, Virtual Edition, is available for Virtual Machine (VM)-based deployment in VMware environments and Microsoft Hyper-V environments.

Polycom supports mixed Hyper-V/VMware environments, but has not tested all configurations and combinations.

Host Installation Guidelines

The following table describes the minimum and maximum VM host requirements for each instance of the RealPresence Access Director, Virtual Edition. The table also shows the typical performance capabilities of each profile.

RealPresence Access Director Deployment Settings in a Virtual Environment Using a 2.9 GHz Server

<i>Component</i>	<i>Minimum Deployment Profile</i>	<i>Maximum Deployment Profile</i>
Virtual Cores*	2	8
CPU	3.5GHz	2GHz
Memory	8 GB	12GB
Storage	146GB	146GB
Number of concurrent calls**	200	1000
Throughput capacity (Mbps)	700	700

* CPU Affinity & HT Sharing should be set to “None.”

** Maximum concurrent call numbers depend on the overall deployment model, network quality, codecs used, total throughput of all calls, and available bandwidth.

Because of differences in hardware and VM environments, the performance information is provided for guidance purposes and does not represent a guarantee of any kind by Polycom.

Hardware Requirements

The following hardware requirements were determined based on test scenarios. Your system’s actual performance may vary based on software or hardware configurations.

To access the management interface, you need a client system running Microsoft® Windows® with the following hardware:

- 1280x1024 (SXGA) minimum display resolution; 1680x1050 (WSXGA+) or greater recommended
- USB and Ethernet ports
- DVD-RW drive or an external DVD burner (Appliance Edition only)

Software Requirements

The following software requirements were determined based on test scenarios. Your system’s actual performance may vary based on software or hardware configurations.

The client system used to access the management interface requires the following software:

- A supported web browser:
 - Microsoft Internet Explorer®, version 10 or later

- Google Chrome™, current version (with Adobe Flash plugin, not built-in Flash support)
- Mozilla® Firefox®, current version
- Java™, version 7
- Adobe® Flash® Player, version 11 or later
For stability and security reasons, Polycom recommends always using the latest version of Adobe Flash Player.

Installation and Upgrade Notes

If you have purchased a new RealPresence Access Director system as a single product or as a component of the RealPresence Clariti solution, see the *Polycom RealPresence Access Director System Getting Started Guide* for instructions on how to install and license your product.

For complete instructions on how to upgrade your system, see the *RealPresence Access Director System Administrator Guide*.

Supported Upgrade Paths

The upgrade package for this software version allows any version 4.1 or 4.2.x RealPresence Access Director system to be upgraded to version 4.2.5. You can download the upgrade package and product documentation from the [RealPresence Access Director support portal](#).

If your system is not currently running version 4.1 or 4.2.x, you need to install intermediate upgrades before upgrading to version 4.2.5. Polycom supports the upgrade paths listed in the following table and recommends that you read all relevant Release Notes before upgrading to an intermediate version.

Upgrade Paths

<i>Current Version</i>	<i>Intermediate Upgrade</i>	<i>Final Version</i>
Prior to version 2.1.x	2.1.x	3.0
3.0		3.1.x
3.1.x	4.0	4.0.1
	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.x		4.1
4.1		4.2.5
4.2.x		4.2.5

Consider the following information if you upgrade from a system running version 4.2.0:

- When you start the upgrade, you will not be logged out of the web user interface immediately. It takes time for the upgrade process to unpack the upgrade file.
- Your browser will lose connectivity to the server during the upgrade and may display an "Unexpected Exception Happened" error or the upgrade status page may lose connectivity to the server. If this happens, let the upgrade proceed.

Upgrading from version 4.1 or 4.2.x to version 4.2.5 can take approximately 45 minutes and require multiple reboots. After you start the upgrade, allow the process to finish. *Do not start an additional upgrade.*

To upgrade to version 4.2.5 of the RealPresence Access Director system:

- 1 Go to **Maintenance > Backup and Restore** and create a new backup of your current system.
- 2 Download the backup file to your local system.
- 3 From the [Polycom Support](#) site, download the appropriate version 4.2.5 upgrade file and save it on your local system:
 - a *.bin file if upgrading from version 4.1
 - b *.upg file if upgrading from 4.2.x
- 4 Follow the instructions in the *Polycom RealPresence Access Director System Administrator Guide* or the online help to upgrade the system to version 4.2.5.

Your browser will lose connectivity to the server during the upgrade and may display an "Unexpected Exception Happened" error or the upgrade status page may lose connectivity to the server. If this happens, let the upgrade proceed.
- 5 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.
- 6 From your browser, log into the system's web interface with the following credentials:
 - User ID: **admin**
 - Password: **Polycom12#\$**
- 7 Go to **Maintenance > Software Upgrade**.
- 8 Review the **System Version** field and **Operation History** table to confirm the upgrade was successful.
- 9 Go to **Admin > Network Settings** and modify your network settings as needed for your environment. *The upgrade may not maintain all network settings.*



Note: If you configured a call policy in the Basic ACL Settings in your previous version of the system, after you upgrade to version 4.2.5, you need to delete your previous settings, disable call policy, re-enable it, and re-configure your previous settings, such as VMR ranges.

Upgrades and Network Interface Mapping in VMware Environments and High Availability Configurations

If you upgrade a VMware instance from version 4.2.x to 4.2.5, eth0 will incorrectly map to network interface 4. However, if you upgrade a VMware instance from version 4.1 to 4.2.5 or install the version 4.2.5 VMware OVA file for the first time, eth0 maps correctly to network interface 1.

If you installed the RealPresence Access Director, Virtual Edition, from the version 4.2.0 OVA file, your Ethernet interface and network adapter mapping may not be sequential due to a known issue in VMware and CentOS. For High Availability configurations in a VMware environment, you need to ensure that both virtual machines have identical sequential Ethernet interface-to-network adapter mapping. If not, you can fix the problem by installing the RealPresence Access Director version 4.2.1 or higher from an OVA file.

Resolved Issues

The following table lists the resolved issues in the RealPresence Access Director system, version 4.2.5.

Resolved Issues

<i>Category</i>	<i>Issue Number</i>	<i>Found in Release</i>	<i>Description</i>
Call Failure	EDGE-1772	4.2.2	When a registered external endpoint calls an external IP address through the RealPresence Access Director system and the RealPresence DMA system successfully resolves the call, the RealPresence Access Director system drops the setup call from the endpoint if the endpoint uses two different IP addresses, one for RAS and one for call signaling. The call is interpreted as a guest call and fails.
H.323 Settings	EDGE-1785	4.2.2	The Classless Internet Domain Routing (CIDR) list for H.323 signaling is limited to 10 records. Note: this version of the RealPresence Access Director system supports 40 records.
Call Failure	EDGE-1885	4.2.3	The RealPresence Access Director system disconnects calls from remote Huawei endpoints.
Two-box Tunnel	EDGE-1909	4.2.4	After disabling the two-box tunnel configuration and restarting the RealPresence Access Director system, a user cannot log in to the web user interface on the management interface IP address and can only log in on the eth0 network interface.
Federations	EDGE-1910	4.2.4	The RealPresence Access Director system does not dial a SIP or H.323 federation based on signaling type but instead dials by the signaling path that was first enabled.
Network Settings	EDGE-1918	4.2.4	Unclear error message displays in the web user interface when configuring network settings with IP addresses already in use.

<i>Category</i>	<i>Issue Number</i>	<i>Found in Release</i>	<i>Description</i>
Call History	EDGE-1925	4.2.3	After calls end, the RealPresence Access Director system does not add media statistics for each call in call history. Note: this version of the RealPresence Access Director system adds media statistics to all calls when the calls end or when a renegotiation of media ports occurs.
Security Settings	EDGE-1933	4.2.5	If you disable TLS 1.0 on the Security page in the web user interface, then upgrade or backup and restore the system, TLS 1.0 is enabled after the upgrade or restore is complete.
Registration	EDGE-1934	4.2.5	The RealPresence Access Director system sometimes reboots automatically, causing registration issues.
SNMP	EDGE-1943	4.2.4	If SNMP is enabled in the RealPresence Access Director system and the system reboots, it no longer responds to SNMP requests. Note: In this version of the RealPresence Access Director system, the external signaling interface can be selected to allow SNMP requests to support load balancers.
SNMP	EDGE-1947	4.2.4	The RealPresence Access Director system only allows SNMP access through the NIC on which the internal management service is assigned.
H.323	EDGE-1948	4.2.4	When using an FQDN as the next hop for H.323, a failure to resolve the name caused the H.323 stack to become unusable.
Two-box Tunnel	EDGE-1949	4.2.4	Cannot log in to the web user interface on the management IP address after disabling two-box tunnel mode and restarting the system.
Upgrades	EDGE-1950	4.1	Upgrades from version 4.0.1 > 4.0 > 4.2.4 fail due to an incorrect routing configuration.
Two-box Tunnel	EDGE-1952	4.2.4	In some two-box tunnel configurations, data packets arrive on the wrong network interface.
Linux	EDGE-1953	4.2.4	The RealPresence Access Director system does not include a Linux crash kernel, which prevents support from obtaining a crash file if the kernel crashes.
Linux	EDGE-1954	4.2.5	Calls through two-box tunnel RealPresence Access Director systems fail due to a Linux kernel crash.
Registration	EDGE-1955	4.2.4	Some HDX endpoints in ITP rooms are unable to register through the RealPresence Access Director system after they crash and reboot during a call. Registration attempts are rejected as duplicates as the system does not correctly time out the previous registrations.

<i>Category</i>	<i>Issue Number</i>	<i>Found in Release</i>	<i>Description</i>
Call Failure	EDGE-1956	4.2.4	Annex O calls to a remote site can fail if the initial LRQ from the RealPresence Access Director system to the remote system fails.
SIP Settings	EDGE-1958	4.2.4	The SIP External Port Settings, Prefix of Userinfo field does not work after upgrading the system to version 4.2.4.

Known Issues

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

Known Issues

<i>Category</i>	<i>Issue No.</i>	<i>Found in Release</i>	<i>Description</i>	<i>Workaround</i>
Certificates	EDGE-1517	4.2.0	An error results when uploading some certificate files due to unsupported characters in the file name.	
Certificates	EDGE-1659	4.2.0	After creating a new SHA-256 Certificate Signing Request (CSR), when you view the CSR by clicking Create a Certificate Signing Request and selecting Use Existing , the system displays a SHA-1 encoded request instead of a SHA-256 request.	<ul style="list-style-type: none"> Go to Admin > Certificates. Click Create a Certificate Signing Request. If a SHA-256 CSR already exists on your system, select Generate New in the Confirm Action window to create a new SHA-256 CSR.
High Availability	EDGE-1600	4.2.0	High Availability settings cannot be configured if two or more network interfaces for the RealPresence Access Director system are not configured consecutively.	Configure network settings on consecutive network interface cards before enabling High Availability. For example, configure network settings for eth0 and eth1 instead of eth0 and eth3, then configure HA settings.

<i>Category</i>	<i>Issue No.</i>	<i>Found in Release</i>	<i>Description</i>	<i>Workaround</i>
High Availability	EDGE-1658	4.2.0	In some situations, after a failover occurs in a High Availability configuration, the RealPresence Access Director system that owns the resources of both systems does not automatically release the resources of the peer system when it requests them.	<p>If resources are not released back to a peer system within a few minutes after it requests them, complete these steps:</p> <ul style="list-style-type: none"> From the web user interface of the system that owns the resources, go to Diagnostics > High Availability Status. Click Release Peer Resources to force the release of the peer system's resources.
Access Control Lists	EDGE-1938	4.2.3.1	When a single Access Control rule includes 15 or more conditions, attempting to edit an existing condition or add a new condition fails.	
Virtual Edition	EDGE-1957	4.2.4	Due to an incompatibility between CentOS 6.8 and VMware tools, deploying and configuring the RealPresence Access Director system from RealPresence Resource Manager or RealPresence Platform Director using an OVA file does not work.	Use VMware VSphere or vCenter to deploy the RealPresence Access Director OVA file. Use the thinshell to configure the network address and then add the instance to RealPresence Resource Manager for licensing.

Get Help

For more information about installing, configuring, and administering Polycom products, refer to the Documents and Downloads section at [Polycom Support](#).

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.

Polycom Solution Support

Polycom Implementation and Maintenance services provide support for Polycom solution components only. Additional services for supported third-party Unified Communications (UC) environments integrated with Polycom solutions are available from Polycom Global Services and its certified Partners. These additional services will help customers successfully design, deploy, optimize, and manage Polycom visual communications within their UC environments.

Professional Services for Microsoft Integration is mandatory for Polycom Conferencing for Microsoft Outlook and Microsoft Office Communications Server or Lync 2010 Server integrations. For additional information, please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Copyright and Trademark Information

Copyright© 2017, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks

Polycom®, the Polycom logo and the names and marks associated with Polycom 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 property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

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.

End User License Agreement

BY USING THIS PRODUCT, YOU ARE AGREEING TO THE TERMS OF THE END USER LICENSE AGREEMENT (EULA) AT: <http://documents.polycom.com/indexes/licenses>. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, DO NOT USE THE PRODUCT, AND YOU MAY RETURN IT IN THE ORIGINAL PACKAGING TO THE SELLER FROM WHOM YOU PURCHASED THE 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.

Customer Feedback

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

Polycom Support

Visit the [Polycom Support Center](#) for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.