# Release Notes

## Polycom® Distributed Media Application™ (DMA®) 7000 System, Version 5.2.2.4

Polycom® announces the release of its Polycom® Distributed Media Application™ (DMA®) 7000 System, version 5.2.2.4. This document provides the latest information about this release.

### Topics



### Copyright Information




3725-76300-001W6 (09/2013)



Polycom Inc.
6001 America Center Drive
San Jose CA 95002 U.S.A.


### Trademark Information

# Introducing the Polycom DMA® 7000 System

The Polycom DMA 7000 system is a highly reliable and scalable video collaboration infrastructure solution. It has two key components, the Conference Manager function and the Call Server function, described below.

Use of this software constitutes acceptance of the terms and conditions of the Polycom DMA 7000 system end-user license agreement on page 37.

### Conference Manager

- Provides a highly reliable and scalable multipoint conferencing solution that distributes voice and video calls across multiple media servers (MCUs), creating a single seamless resource pool. The system essentially behaves like a single large MCU, which greatly simplifies video conferencing resource management, improves efficiency, and facilitates ad hoc (reservationless) conferencing.
- Supports up to 64 MCUs and 1200 concurrent conference (virtual meeting room, or VMR) calls.
- MCUs can be added on the fly without impacting end users and without requiring re-provisioning.

### Call Server

- Provides complete endpoint registration and call routing services for both H.323 and SIP protocols.
- Also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to begin transitioning to the use of SIP in a gradual, orderly, and cost-effective manner.
- Provides bandwidth management, including tracking resource usage and controlling excessive resource usage.
- Can be integrated with a Juniper Networks Session and Resource Control Module (SRC) that provides bandwidth assurance services.
- Comes with a default dial plan that covers many common scenarios, but which can be modified in a simple, but powerful and flexible, way.

The Call Server makes it possible for multiple UC environments and different video conferencing technologies to be unified across the network into a single dial plan.

### Clustering and Superclustering

The Polycom DMA system can be configured as a *cluster* of two co-located servers, providing a highly reliable system with no single point of failure. It can also be deployed as a *supercluster* of up to five geographically dispersed, but centrally managed, DMA system clusters (two-server or single-server) to provide even greater reliability, geographic redundancy, and better network traffic management. Up to three of the clusters in a supercluster can have Conference Manager enabled.

The clusters in a supercluster share a common data store. Each cluster maintains a local copy of the data store, and changes are replicated to all the clusters.

A five-cluster supercluster supports up to 25,000 concurrent calls and 75,000 registrations.

### Other Key Features

The Polycom DMA 7000 system also:

- Integrates with Microsoft Active Directory, automating the task of provisioning users for video conferencing. Combined with its advanced resource management, this makes ad hoc video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.
- Integrates with Microsoft Exchange Server, enabling users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.
- Integrates with a Polycom RealPresence Resource Manager or CMA system to obtain site topology and user-to-device association data.
- Includes the RealPresence Platform Application Programming Interface (API), which provides programmatic access to the Polycom DMA system for the following:
  - Provisioning
  - Conference control and monitoring
  - Call control and dial-out
  - Billing and usage data retrieval
  - Resource availability queries

  The API uses XML encoding over HTTPS transport and adheres to a Representational State Transfer (REST) architecture.

  The RealPresence Platform API is licensed separately for use by third-party client applications.

*A Polycom RealPresence Resource Manager system can access the API without needing an API license. An API license is only needed if a client application that you or a third party develop is going to access the API.*

- SNMP support

  An SNMP agent provides access to MIBs for the DMA application, CentOS operating system, Java Virtual Machine, and server hardware, enabling your network management system to monitor the Polycom DMA system and receive notifications (traps and informs).

  The system supports SNMPv3 communications with authentication and privacy.

### System Capabilities and Constraints

The following capabilities and constraints apply to the entire supercluster:

- Number of sites: 500
- Number of subnets: 5000
- Number of clusters in a supercluster: 5 (not counting an integrated Polycom RealPresence Resource Manager or CMA system)
- Number of MCUs enabled for conference rooms: 64
- Number of territories enabled for conference rooms (Conference Manager enabled): 3
- Number of concurrent VMR calls: 1200 per cluster (Conference Manager), up to 3600 total
- Number of concurrent SIP<->H.323 gateway calls: 500

- Size of Active Directory supported: 1,000,000 users and 1,000,000 groups (up to 10,000 groups may be imported)

The following capabilities and constraints apply to each cluster in the supercluster:

- Number of registrations: 15000
- Number of concurrent H.323 calls: 5000
- Number of concurrent SIP calls: 5000
- Total number of concurrent calls: 5000
- Number of network usage data points retained: 8,000,000
- Number of IRQ messages sent per second: 100
- Maximum number of history records retained per cluster (lower limits can be set on the History Retention Settings page):
  - 500,000 registration history
  - 2,000,000 registration signaling
  - 500,000 call history
  - 200,000 conference history

# What's New in the Version 5.2.2.4 Release

The Polycom DMA system version 5.2.2.4 is a maintenance release that addresses some issues found since the previous version 5.2.2 releases and replaces those releases.

### Issues Resolved in Version 5.2.2.4

The following table lists the issues resolved in version 5.2.2.4.

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-11938 | 5.2.2.2 | A Codian MCU, acting as an ISDN-to-H.323 gateway, sent a call with a null calling party number (caller ID) to the DMA system. The DMA system terminated all subsequent calls from the Codian MCU. |
| DMA-11911 | 5.2.2.2 | On the History Retention Settings page, **Include keep-alive messages in registration history** was not selected, but outbound registration keep-alive messages were retained anyway. |
| DMA-11910 | 5.2.2.3 | Dial rule preliminary scripts containing certain variables were always reported as having a compilation error. If saved anyway, they were disabled. |
| DMA-11886 | 6.0.2 | Errors with log file operations were not being recorded in the server log file. |
| DMA-11871 | 5.2.2.3 | In the Select Layout dialog box for conference templates, some of the layouts were incorrectly identified. |
| DMA-11824 | 5.2.2.2 | If the DMA system was registered with a SIP peer, its registration refresh (keep-alive) messages to the SIP peer appeared in Registration History as timeouts. |
| DMA-11815 | 5.1, 5.2.2.2, 6.0.2 | H.323 VMR calls from the internet could be routed to the wrong MCU due to improper parsing of the h323CallSignalAddress. |

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-11801 | 5.2.2.2 | In a two-server cluster, the servers refresh their cached conference room data every 15 seconds. Whenever the data changed, a short-lived alert 3605 could occur because one server's cache was refreshed just before the change. The alert is now triggered only if the conference room counts differ for two refresh intervals in a row. |
| DMA-11797 | 5.1.0 P1, 5.2.2, 6.0.2 | When an H.323 endpoint sent a registration request (RRQ) followed immediately by an unregistration request (URQ), and then sent another RRQ, the endpoint's registration was left in a bad state. |
| DMA-11787 | 6.0.2 | When conference rooms are created in the management interface, the DMA system does a case-insensitive check for conference ID uniqueness (for instance, Test and teSt are considered duplicates). But via the API, the DMA system failed to do a case-insensitive check, so it was possible to start two conferences using the conference IDs Test and teSt. |
| DMA-11781 | 5.2.2, 6.0.2 | During startup of a two-server cluster, core DMA processes sometimes started prior to completion of data synchronization between the two servers. This caused repeated restarts of the cluster and delays in achieving an operational state. |
| DMA-11774, DMA-11752, DMA-11750 | 5.2.2.2 | Under certain circumstances, dynamically managed endpoints communicating through a VBP session border controller consumed multiple licenses from the RealPresence Resource Manager system. This was caused by the DMA system improperly associating signaling events to the endpoints. |
| DMA-11734 | 5.2.2.2 | When dialing out via RealPresence Access Director in order to add an external H.323 guest endpoint to a conference, the DMA system set the destination call signaling address to the IP address of the RealPresence Access Director system, causing the call to fail. |
| DMA-11716 | 5.2.2 | When using a "Resolve to external address" dial rule to resolve an H.323 URL, the DMA system performed SRV queries it shouldn't have. This resulted in calls to external endpoints failing. |
| DMA- 11319 | 5.2.1 | The DMA system doesn't support H.245 encapsulation or FastConnect. But when an endpoint sends a startH245 Facility message, the system passes that message on to the MCU hosting the conference. VVX 1500 endpoints were sending such a message. The issue is resolved by a VVX configuration change; the DMA system is working as designed. |
| DMA-10111 | 5.2 | RMX MCUs have a per-conference limit of 160 (MPM+ cards) or 180 (MPMx cards) participants. A conference with large numbers of CIF participants could reach this limit and still have capacity available. The DMA system saw capacity still available on the current MCU, so rather than create a cascade link to another MCU, it continued to send calls to current one. These calls were rejected. |
| DMA-8305 | 5.0 | An RMX MCU was configured with both video and audio ports, and the DMA system was configured to reserve video ports on the MCU for use by the CMA system. The DMA system failed to honor the port reservation and used video ports reserved for the CMA system. |

## Issues Resolved in Version 5.2.2.3

The following table lists the issues resolved in version 5.2.2.3.

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-11714 | 5.2.2.2 | Calls from a site that allows internet SIP calls via a session border controller (SBC) were not routed to the SBC. |
| DMA-11667 | 5.2.2.2 | In the Dial-out Presets section of the Add/Edit Conference Room dialogs, the IVR DTMF field didn't accept the star (*) as a valid DTMF key. |
| DMA-11634 | 5.2.2.2 | Assigning a conference passcode to an AD user's conference room (VMR) failed unless a chairperson passcode was also assigned. |
| DMA-11627 | 5.2.2.2 | Dial rule preliminary scripts couldn't be successfully saved after editing. |
| DMA-11617 | 5.2.2 | Calls remained on the Active Calls page after they were terminated. |
| DMA-11586 | 5.2.2.2, 6.0.2 | When CDRs were exported from a supercluster for a time period known to include calls, the files were empty. |
| DMA-11567 | 5.1, 5.2, 6.0 | A race condition between the thread joining a call to conference and the thread reading the conference and participant information from the MCU sometimes led to termination of the call. |
| DMA-11565 | 5.1.0 P1 HF1 | API calls to mute or unmute a participant in a secured conference failed, and the unmute command disconnected the participant. |
| DMA-11559 | 5.2, 6.0 | Transfer of site link throttlepoint data across clusters failed. |
| DMA-11548 | 5.0.2 P1 | An API call to mute a participant in a cascaded conference resulted in the participant's mute state repeatedly flip-flopping. |
| DMA-11543 | 5.1, 5.2.2 P1 | The DMA system failed to prefer SVC-capable MCUs when routing calls to a Mixed AVC and SVC mode conference. |
| DMA-11523 | 5.2.2.2 | On Dell R620 servers, the SNMP agent failed to send hardware MIB traps. |
| DMA-11501 | 5.1.0 P1 HF1 | For a very large RealPresence Resource Manager scheduled meeting (around 400 endpoints in conference), the DMA system was sending so many API notification events to the RealPresence Resource Manager system that the conference end notification didn't arrive for more than ten minutes. |
| DMA-11440 | 5.2.1 | The DMA system accepted and attempted to use an invalid dial rule preliminary script, causing all calls to fail. |
| DMA-11417 | 5.2.2 P1 | After a PFX file containing a PKCS12 keystore with a blank password was uploaded, the DMA system's management interface became inaccessible. |
| DMA-11383 | 5.2.2 | Following an upgrade from 5.2.0, the DMA system software failed to start after a reboot. |
| DMA-11382 | 5.2.2 | After using the USB Configuration Utility to reconfigure a single-server system to two-server configuration, the DMA system software failed to start until after second reboot. |
| DMA-11381 | 5.2.2 | Following an upgrade from 5.2.0, some configuration data related to virtual entry queues was lost. |
| DMA-11380 | 5.2.2 | Attempt to add a second server to a single-server DMA system failed. The new server didn't see the existing server on the private network connection. |
| DMA- 11363 | 5.2 | If **Allow calls to/from rogue endpoints** was turned off on the **Call Server Settings** page, calls to endpoints registered to a different cluster in the supercluster failed. |
| DMA-11360 | 6.0.2 | SIP failure code messages were truncated in CDRs. |

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-11346 | 5.2 | Both servers of a two-server cluster attempted to register with an external SIP peer at the same time. |
| DMA-11285 | 5.2 | The DMA system intermittently lost connection to a Cisco MSE 8000 MCU. |
| DMA-11265 | 5.2.1 | Deadlocked SIP threads sometimes caused SIP calls and registrations to fail. |
| DMA-11196 | 5.1 | After a network outage caused a two-server cluster to lose connection to most of its MCUs, it became unstable and unresponsive. Both servers had to be rebooted. |
| DMA-11168 | 5.0.2 P1 HF1 | When the DMA system was in direct mode, calls from an endpoint behind a VBP or on a neighbored system to another endpoint behind a VBP or on a neighbored system, or to a VMR on a neighbored system, could remain in the Active Calls list indefinitely. |
| DMA-11056 | 5.1.0 P1 | Disconnecting and reconnecting the primary LAN cable on the standby server of a two-server cluster caused the virtual IP to fail over, and some calls were dropped. |
| DMA-11036 | 6.0.1 | For a SIP dial-out call to a Lifesize endpoint, the dialString and destEndpoint fields in the CDR were truncated. |

## Feature Enhancements in Version 5.2.2.2

The Polycom DMA system version 5.2.2.2 included the feature enhancements described below.

- API changes

  The RealPresence Platform API included in this release contains new versions of some objects (such as plcm-conference-template). To maintain backward compatibility, previous versions of those objects remain available. For all GET requests, API clients should use the Accept header to specify the version of the object that the client can handle. For instance, depending on the API version for which the client was written, the Accept header for a conference template request might be one of the following:

  - "application/vnd.plcm.plcm-conference-template+xml"
  - "application/vnd.plcm.plcm-conference-template-v2+xml"
  - "application/vnd.plcm.plcm-conference-template-v3+xml"

  Failure to include an Accept header may result in a random version being sent. Refer to the API documentation for more information about the Accept header and the available versions.

- Greatly simplified History Retention Settings page

  Changes to the management of database table sizes and record purging have led to the removal of all configuration settings specifying the number of records of various types to be retained. The only configuration options remaining are:

  - Whether to retain Call Server registration history records.
  - If retaining registration history, whether to include keep-alive messages.
  - How many repeated low-value signaling messages (such as INFO messages about in-call status) to retain for a given call.

### Issues Resolved in Versions 5.2.2.0 - 5.2.2.2

The following table lists the issues resolved in versions 5.2.2.0 - 5.2.2.2.

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-11485 | 5.2.1 | The system failed to properly handle SUBSCRIBE session setup and termination, leading to high CPU usage, memory errors, and resulting functionality problems. |
| DMA-11474 | 5.2.2.1 | After the system was upgraded from 5.2.2 to 5.2.2.1, call history was missing. |
| DMA-11430 | 5.1 | When the DMA system attempted to retrieve endpoint information from a RealPresence Resource Manager system that was very slow or unresponsive, it stopped responding to RRQs and other RAS messages. |
| DMA- 11389 | 5.2.2 | When upgrading to 5.2.2 from 5.2.0 or 5.2.1, in some circumstances the data in the PostgreSQL database was lost. |
| DMA-11337 | 5.0.2 P1 HF1 | When an API client that's subscribed to conference notifications failed to respond to a notification, the DMA system waited indefinitely. Subsequent notifications to that client were queued up without limit, consuming large amounts of memory.<br>Now, the system discards a notification if it receives no response within 10 seconds, and it sends the next notification in the client's queue.<br>The notification queue for a client is now limited to 500. If it reaches that limit, the system discards the oldest notification in the queue. |
| DMA-11196 | 5.1 | After a network outage caused a two-server cluster to lose connection to most of its MCUs, it became unstable and unresponsive. Both servers had to be rebooted. |
| DMA-11212 | 5.0 | OpenDJ (LDAP directory service used for sharing data across a supercluster) locked up during network outage. |
| DMA-11150 | 5.0.2 | The system took 60 seconds or more to respond to LWRRQs (light-weight registration requests). |
| DMA-11146 | 6.0.0 | The system experienced long pauses (up to 30 seconds) due to virtual memory thrashing and 100% disk usage. |
| DMA-11100 | 5.2.1 | Upgrade from 5.0.1 to 5.2.1 left system in an inconsistent state. |
| DMA-11085 | 5.2.2 | Install of 5.2.2 failed. |
| DMA-11025 | 5.0 | Log rolling failed and no log archive was created. |
| DMA-11019 | 5.0 | The Shutdown and Restart page didn't provide a way to restart one server of a two-server cluster. |
| DMA-11013 | 5.2.0 | Calls from an unregistered ITP room to a DMA-registered ITP room resulted in only the primary endpoint (codec) connecting. |
| DMA-10925 | 5.1.0 P1 | The servers in a two-server cluster battled over which was the active server, causing their roles to switch back and forth repeatedly. |
| DMA-10894 | 5.0 | Database audit purge continued to purge after it should have stopped. |
| DMA-10884 | 6.0.1 | Anonymous users could access the LDAP database via port 4449 and access configuration and user data for the system. |
| DMA-10729, 10348 | 5.2 | A two-server cluster sometimes experienced data synchronization issues in reboot or failover situations. |
| DMA-10721 | 5.1 | RealPresence Resource Manager reported that the DMA system was down when it was operational with no issues. |

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-10636, 9312 | 5.0 | If either (a) the active server in a two-server cluster failed over to the backup server or (b) the primary cluster for a territory failed over to the backup cluster, a conference for which the failed server or cluster was responsible could continue without the backup server or cluster taking over signaling for it. If a new (or dropped) participant dialed into the same conference room (VMR), the backup server or cluster started a new conference. This resulted in two active conferences for the same VMR.<br>To prevent such split conferences, when a server or cluster fails, the backup server or cluster contacts the MCU(s) to terminate the conferences for which the failed server or cluster was responsible (this may take up to two minutes).<br>**Note:** Depending on the endpoint, when the conference is terminated, the endpoint's video may freeze instead of the call hanging up. The user can simply hang up and dial back in.<br>When the participants in a conference dial back in, the backup server or cluster creates a new conference.<br>**Note:** Some calls killed in this way may continue to appear on the Active Calls page for up to 30 minutes, depending on the number of such calls.<br>Also fixed in 5.0.2.1. |
| DMA-10208 | 5.2 | In a two-server cluster running on Dell R620 servers, the private network connection between the two servers randomly failed. |

## Issues Resolved in Version 5.2.1

The following table lists the issues resolved in the version 5.2.1 release.

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-10561 | 5.2 | The system leaked memory when an API client used certain conference commands. |
| DMA-10520 | 5.0.1 HF1 | When DMA is neighbored to Avaya Communication Manager, H.323 calls from an RMX registered to the DMA to an Avaya Meeting Exchange failed to connect. |
| DMA-10508 | 4.0.3 | Audio dial-in over a SIP trunk failed to connect to the VMR of the destination conference. The call connected to the RMX MCU for the initial VEQ greeting, but was dropped when the VMR number was entered. |
| DMA-10488 | 5.2 | Destination of point-to-point calls was not recorded in call history. |
| DMA-10482 | 5.2 | When SIP VMR calls requested more bandwidth than available, the DMA system failed to properly downspeed them. Instead, the calls were shown in the MCU as connected with problems and they failed to get video. |
| DMA-10468 | 5..2 HF2 | For all point-to-point calls and some VMR calls, the system leaked memory in the call audit cache. |
| DMA-10444 | 5.1.0 P1 HF1 | When the hub MCU of a cascaded conference became unavailable, the cascade link remained active for around 15 minutes. |
| DMA-10430 | 5.2 | Point-to-point SIP calls failed for endpoints that register a contact URI without port, such as the LifeSize Team 220. |
| DMA-10404 | 5.2 | SIP TLS calls to a Cisco 4505 MCU failed. |
| DMA-10380, 10381 | 5.0.1, 5.1, 5.2 | The DMA system failed to check a registration policy script for syntax errors before saving. When it tried to apply the script, all MCU registrations failed. |
| DMA-10368 | 5.2 | Attempt to restore a two-server cluster from a backup failed. |

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-10314 | 5.2 | If a non-numeric conference room was used, SVC endpoints weren't notified of all the media streams and effectively received a video switching (VSW) experience. |
| DMA-10303 | 5.2 | When an endpoint that doesn't support encryption called a VEQ in order to join a conference configured to "encrypt when possible," the transfer from the entry queue to the destination conference failed. |
| DMA-10301 | 5.0.2 | The upgrade process did not migrate user roles assigned to imported AD groups. |
| DMA-10231 | 5.2 | A memory leak in the handling of SIP SVC calls caused a DMA server failover. |
| DMA-10212 | 5.2 | H.323 Annex O dial-outs from a VMR to an external address weren't routed to the VBP as specified in the internet call routing configuration and thus failed. |
| DMA-10198 | 5.0.2 | When an ISDN endpoint called a VMR hosted on the same MCU whose ISDN gateway the call was using, the DMA system detected this as a loop, and the call failed. |
| DMA-10196 | 5.1.0 P1 | When the hub MCU of a cascaded conference became unavailable, the cascade links from spoke MCUs remained active. H.323 endpoints that were on the hub MCU couldn't dial back into the conference and hub failover didn't happen. |
| DMA-10195 | 5.1 | Searching registration history caused high CPU usage, triggering an alert. |
| DMA-10124 | 5.0.1 | Chairperson passcodes couldn't be added or edited in the Edit User dialog. |
| DMA-9931, 10023, 10026 | 5.2 | MCU failover didn't work for SVC calls or for AVC calls on RealPresence Collaboration Server 800s MCUs. |
| DMA-6728 | 4.0 | The Network Usage page showed incorrect packet loss data. |

## What's New in the Version 5.2 Release

The Polycom DMA system version 5.2 includes the following new features. For more information on these new features, see the *Polycom DMA 7000 System Operations Guide* and the online help.

- Cascading for size

  This version of the Polycom DMA system supports a new method of cascading a conference across multiple MCUs that makes it possible for a conference to contain many more participants than there is room for on any single MCU. Cascading for size requires Polycom MCUs.

  Cascading for size and cascading for bandwidth are two separate and mutually exclusive options. Cascading for size is best suited to presentation-style conferences where only a few participants speak and everyone else only listens.

- Support for Polycom RealPresence Collaboration Server MCU

  This version of the Polycom DMA system supports the new RealPresence Collaboration Server 800s MCU.

- Support for mixed AVC and SVC conferences

  A new conference mode setting on conference templates, **Mixed AVC and SVC**, supports the ability of Polycom RealPresence Collaboration Server 800s MCUs to host SVC and AVC calls in the same conference (VMR).

  When mixed mode is specified and an MCU that supports it is selected for the conference, both SVC and AVC endpoints can join the conference, and each gets the appropriate experience: SVC endpoints get SVC mode and get a video stream for each AVC participant; AVC endpoints get a

single Continuous Presence (CP) video stream of the participants (both AVC and SVC) supplied by the MCU.

RealPresence Collaboration Server 800s MCUs don't currently support video switching mode for mixed SVC and AVC conferences, and Video Switching should not be selected in mixed mode conference templates.

---

*If the conference template selected for a conference specifies mixed AVC and SVC mode, the DMA system doesn't limit the choice of MCU to those that support mixed mode.*

*If the MCU selected doesn't support SVC at all, the DMA system starts the conference as an AVC-only conference. Otherwise, it starts a mixed mode conference.*

*If the MCU supports SVC-only conferences, but not the mixed AVC and SVC mode specified in the template, the conference simply doesn't start.*

*Use appropriately configured MCU pools and pool orders to limit mixed-mode conferences to MCUs that support mixed AVC and SVC mode.*

---

- Firewall/NAT traversal keep-alive support

  On the latest Polycom RMX and RealPresence Collaboration Server MCUs, conferences can be configured to send media stream keep-alive messages to an SBC for calls received from the SBC. This version of the Polycom DMA system supports this feature with two new conference mode settings on conference templates, **FW NAT keep alive** and **Interval**.

- Subscription Events tab added to Call Details dialog box

  The call history includes records of the SIP SUBSCRIBE/NOTIFY signaling messages (RFC 4575 notifications) by which conference participants subscribe to a conference and receive notifications of conference events. In version 5.1, these records appeared in the **Call History** list as separate "calls." These records are now displayed on the new **Subscription Events** tab of the **Call Details** dialog box for the call with which they're associated.

---

*Although the system can be configured to allow non-conference participants to subscribe to conference events, the call history doesn't include SUBSCRIBE/NOTIFY signaling messages for non-conference participants.*

---

- New API functionality

  In this version of the Polycom DMA system, the RealPresence Platform Application Programming Interface (API) includes create, read, update, and delete (CRUD) control of MCUs.

- CDR time/date format change

  The format of the startTime and endTime fields in call detail records has been changed to:

  `YYYY-MM-DDTHH:MM:SS.FFF[+|-|Z][HH:MM]`
  (where FFF is milliseconds and Z is zero offset)

- XMPP chat and presence services removed

  The XMPP server that could be enabled in prior versions of of the Polycom DMA system is no longer available.

### Server Change for New System Installations

The Dell server used for new DMA system installations has changed from the PowerEdge R610 to the PowerEdge R620 server. In general, this change is transparent to customers, with one exception: a monitor and USB keyboard are required to run the Dell server diagnostic utilities on the R620 server.

Please note:

- Earlier versions of the DMA system software have not been tested and so are not supported on the R620 server.
- The Dell server diagnostic utilities are to be used only under the direction of Polycom Global Services.

## Software Version History

Only versions released for General Availability are listed.

| Version | Release Date | Features |
|---|---|---|
| 6.0.2.1 | August 2013 | Maintenance release to fix specific issues. |
| 5.2.2.3 | August 2013 | Maintenance release to fix specific issues. |
| 6.0.2 | July 2013 | DMA-controlled IVR services for VEQs with custom prompt sets and operator assistance, call/conference history and CDR enhancements, AS-SIP resource priority support, gatekeeper blacklist, management connection whitelist, ANAT support, individual server shutdown/restart. |
| 5.2.2.2 | July 2013 | Maintenance release to fix specific issues. |
| 5.2.2 | June 2013 | Maintenance release to fix specific issues. |
| 5.2.1 | March 2013 | Maintenance release to fix specific issues. |
| 5.2.0 | December 2012 | Cascading for size, mixed AVC/SVC conferences, FW NAT keep-alive, improved subscription events reporting, new MCU support, enhanced API control of MCUs, removal of XMPP server. Database changed from MySQL to PostgreSQL 9.2.1. |
| 5.0.2 | December 2012 | Maintenance release to fix specific issues. |
| 5.1.0_P1 | December 2012 | Maintenance release to fix specific issues. |
| 5.1.0 | November 2012 | SVC conferencing, RFC 4575 support, untrusted traffic identification and handling, network setting changes, upgrade process monitoring, configuration-only backups. |
| 5.0.1 | September 2012 | Maintenance release to fix specific issues. |
| 4.0.3_P4 | August 2012 | Maintenance release to fix specific issues. |
| 5.0.0 | July 2012 | RealPresence Platform API, SNMP support, device authentication enhancements, SIP enhancements, log forwarding, ITP support enhancements, performance improvements. |
| 4.0.3_P3 | July 2012 | Maintenance release to fix specific issues. |
| 4.0.3_P2 | July 2012 | Not released for General Availability. |
| 4.0.3_P1 | May 2012 | Maintenance release to fix specific issues, plus new call server option and subnet naming. |
| 4.0.3 | March 2012 | Maintenance release to fix specific issues, plus authentication, SIP peer and endpoint enhancements, AD integration and database performance improvements, and new registration policy script variable. |

| Version | Release Date | Features |
|---|---|---|
| 4.0.2 | February 2012 | Maintenance release to fix specific issues. |
| 4.0.1 | December 2011 | Maintenance release to fix specific issues. |
| 4.0.0 | October 2011 | Registration control, GK IPv6 support, Dashboard enhancements, SIP interoperability enhancements, maximum security mode. |
| 3.0.0_P1 | September 2011 | Maintenance release to fix specific issues. |
| 3.0.0 | July 2011 | Call Server, superclustering, Juniper SRC integration, new Dashboard, new reporting and monitoring pages, new licensing. |

## The Consequences of Enabling Maximum Security Mode

Enabling the **Maximum security** setting is ***irreversible*** and has the following significant consequences:

- All unencrypted protocols and unsecured access methods are disabled.
- The boot order is changed and USB ports are disabled so that the server(s) can't be booted from the optical drive or a USB device.
- A BIOS password is set.
- The port 443 redirect is removed, and the system can only be accessed by the full URL (https://<IP>:8443/dma7000, where <IP> is one of the system's management IP addresses or a host name that resolves to one of those IP addresses).
- For all server-to-server connections, the system requires the remote party to present a valid X.509 certificate. Either the Common Name (CN) or Subject Alternate Name (SAN) field of that certificate must contain the address or host name specified for the server in the Polycom DMA system.

  Polycom RealPresence Collaboration Server and RMX MCUs don't include their management IP address in the SAN field of the CSR (Certificate Signing Request), so their certificates identify them only by the CN. Therefore, in the Polycom DMA system, an RMX MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by the IP address.

  Similarly, an Active Directory server certificate often specifies only the FQDN. So, in the Polycom DMA system, identify the enterprise directory by FQDN, not by the IP address.
- SIP signaling is not supported.
- Superclustering is not supported.
- The Polycom DMA system can't be integrated with Microsoft Exchange Server and doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.
- Integration with a Polycom RealPresence Resource Manager or CMA system is not supported.
- On the **Banner** page, **Enable login banner** is selected and can't be disabled.
- On the **Login Sessions** page, the **Terminate Session** action is not available.
- On the Troubleshooting Utilities menu, Top is removed.
- In the **Add User** and **Edit User** dialog boxes, conference and chairperson passcodes are obscured.
- After **Maximum security** is enabled, management interface users must change their passwords.

- If the system is not integrated with Active Directory, each local user can have only one assigned role (Administrator, Provisioner, or Auditor).

  If some local users have multiple roles when you enable the **Maximum security** setting, they retain only the highest-ranking role (Administrator > Auditor > Provisioner).

- If the system is integrated with Active Directory, only one local user can have the Administrator role, and no local users can have the Provisioner or Auditor role.

  If there are multiple local administrators when you enable the **Maximum security** setting, the system prompts you to choose one local user to retain the Administrator role. All other local users, if any, become conferencing users only and can't log into the management interface.

  Each enterprise user can have only one assigned role (Administrator, Provisioner, or Auditor). If some enterprise users have multiple roles (or inherit multiple roles from their group memberships), they retain only the lowest-ranking role (Administrator > Auditor > Provisioner).

- Local user passwords have stricter limits and constraints (each is set to the noted default if below that level when you enable the **Maximum security** setting):

  - Minimum length is 15-30 characters (default is 15).
  - Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).
  - Maximum number of consecutive repeated characters is 1-4 (default is 2).
  - Number of previous passwords that a user may not re-use is 8-16 (default is 10).
  - Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).
  - Password may not contain the user name or its reverse.
  - Maximum password age is 30-180 days (default is 60).
  - Minimum password age is 1-30 days (default is 1).

- Other configuration settings have stricter limits and constraints (each is set to the noted default if below that level when you enable the **Maximum security** setting).

  Session configuration limits:

  - Sessions per system is 4-80 (default is 40).
  - Sessions per user is 1-10 (default is 5).
  - Session timeout is 5-60 minutes (default is 10).

  Local account configuration limits:

  - Local user account is locked after 2-10 failed logins (default is 3) due to invalid password within 1-24 hours (default is 1).
  - Locked account remains locked either until unlocked by an administrator (the default) or for a duration of 1-480 minutes.

- Software build information is not displayed anywhere in the interface.

- You can't restore a backup made before the **Maximum security** setting was enabled.

- File uploads may fail when using the Mozilla Firefox browser unless the proper steps have been taken. See the *Polycom DMA 7000 System Deployment Guide for Maximum Security Environments*, the *Polycom DMA 7000 System Operations Guide*, or the online help.

## System Requirements

- For best reliability, deploy the Polycom DMA 7000 system into a good-quality IP network with low latency and very little packet loss.
  - In systems with Active Directory integration, the network between the DMA system and Active Directory should have less than 200 ms round-trip latency and less than 4% round-trip packet loss.
  - The network between clusters of a Polycom DMA supercluster should have less than 200 ms round-trip latency and less than 2% round-trip packet loss.
  - The network between the Polycom DMA system and all MCUs should have less than 200 ms round-trip latency and less than 2% round-trip packet loss. Since this network carries only signaling traffic (the RTP stream goes directly from the endpoint to the MCU), bandwidth is not an issue.
  - The network between the Polycom DMA system and video endpoints should have less than 200 ms round-trip latency and less than 6% round-trip packet loss.
- Computers used to access the management interface should have 1280x1024 minimum display resolution (wide screen, 1680x1050 or greater, recommended).
- Browser minimum requirements: Microsoft Internet Explorer® 7.0, Mozilla Firefox® 3.0, or Google Chrome 11 (with Adobe Flash plugin, not built-in Flash support).

*The Polycom DMA system's management interface requires Adobe Flash Player. For stability and security reasons, we recommend always using the latest version of Flash Player.*

## Installation and Upgrade Notes

### New System Installation

Installation of new Polycom DMA 7000 systems is managed through Polycom Global Services. For more information, please contact your Polycom sales or support representative.

See the *Deploying Visual Communications Administration Guide* for detailed installation requirements and information.

### Existing System Upgrade

Polycom DMA systems running versions 5.0 or 5.1 (with or without service packs or patches) can be upgraded to version 5.2.2.3. This upgrade requires a new license key after the upgrade.

Polycom DMA systems running version 4.x must be upgraded to version 5.0 or 5.1 before being upgraded to version 5.2.2.3.

*See "DNS Records Requirement Changes" and, if applicable, "Version 5.0 to 5.1 IP Addressing Change" on page 16 regarding configuration changes you may need to make before proceeding.*

Polycom DMA systems running version 5.2.0, 5.2.1, or previous version 5.2.2.x releases can be upgraded without requiring a new license key.

*After upgrading to version 5.2.2.3, rolling back to version 5.2.0 or 5.2.1 is not possible.*

*As a workaround for certain issues in versions 5.2.0 and 5.2.1 (such as DMA-10729 and DMA-10208), some customers were advised to shut down the second server of a two-server cluster. To upgrade such a system to version 5.2.2.3, see "Upgrading a Cluster with One Server Disabled" on page 17.*

See the *Polycom DMA 7000 System Operations Guide* and online help for upgrading and licensing procedures.

### Version 5.0 to 5.1 IP Addressing Change

Prior to version 5.1, a single-server DMA system had two host names and two IP addresses (plus two more of each for the signaling network in split network configuration), a physical host name and IP address and a virtual host name and IP address. Beginning with version 5.1, a single-server system no longer has a virtual host name and IP address. All references to the system use the physical host name and physical IP address. (Exception: If only IPv6 is enabled, the system must have two addresses, so a single-server IPv6-only system must still have a virtual host name and IP address.)

When a single-server version 5.0 DMA system with IPv4 enabled is upgraded to version 5.2, the previous version's virtual host name(s) and IP address(es) become the upgraded version's physical host name(s) and IP address(es). This is done because in prior versions, all access to the DMA system was supposed to use the virtual host name or IP address. Using the previous version's virtual host name(s) and IP address(es) as the new physical host name(s) and IP address(es) ensures that external devices can access the system without having to be reprovisioned.

*Whether the virtual host name(s) and IP address(es) are required depends on the **System server configuration** setting. If a single-server DMA system is configured as a two-server system (not recommended and not supported), it continues to require the virtual host name(s) and IP address(es).*

### DNS Records Requirement Changes

Prior to version 5.2, enterprise DNS A/AAAA records for the physical host names of the DMA system were optional, but strongly recommended, and the NS records needed to support the Embedded DNS feature identified the DMA system's embedded DNS servers by their virtual host names. Version 5.2 requires the following changes:

- A/AAAA records for both the physical and virtual host names are mandatory.
- The Embedded DNS feature requires a DNS NS record for the physical host name of each server in each cluster in the supercluster.
- NS records for the virtual host names must not exist.

See "Add Required DNS Records for the Polycom DMA System" in the *Polycom DMA 7000 System Operations Guide* and online help for details.

### Upgrading a Cluster with One Server Disabled

To upgrade a version 5.2.0 or 5.2.1 two-server cluster that has one server shut down due to issues in those versions:

1. Leave Server B (the shut-down server) turned off.
2. Upgrade Server A (the running server) as described in the *Polycom DMA 7000 System Operations Guide* and online help.
3. When the Server A upgrade and reboot are finished, log back in, go to **Maintenance > Shutdown and Restart**, and shut down Server A.
4. Once Server A is shut down, turn on Server B.
5. Upgrade Server B as described in the *Polycom DMA 7000 System Operations Guide* and online help.
6. When the Server B upgrade and reboot are finished, log back in, go to **Maintenance > Shutdown and Restart**, and shut down Server B.
7. Turn on Server A and wait for it to finish booting and display **DMA Ready** on the LCD (about five minutes).
8. Turn on Server B.

   Server B boots, detects the presence of Server A, gets its configuration settings from it, synchronizes its data, and joins the cluster. When done, both servers' LCDs display **DMA Clustered**.

## 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 Server integrations. For additional information, please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

## Interoperability

### Integration with Polycom RMX™ 1500/2000/4000 MCUs

To support the Polycom DMA system's **High security** setting, configure the Polycom RMX MCUs being added to the system to accept encrypted (HTTPS) management connections.

The Polycom DMA system uses conference templates to define the conferencing experience associated with a conference room or enterprise group. Conference templates can be free-standing or linked to an RMX conference profile. If you link templates to RMX profiles, make sure the profiles exist and are defined the same on all the Polycom RMX MCUs that the Polycom DMA system uses.

Refer to the *Polycom DMA 7000 System Operations Guide* or online help for more information on setting up MCUs for the Polycom DMA system. Refer to the *Polycom RMX Administrator's Guide* for more information on enabling encrypted connections and creating RMX profiles.

*In order to efficiently manage multiple calls as quickly as possible, the Polycom DMA system uses multiple connections per MCU. By default, an RMX MCU allows up to 20 connections per user (the MAX_NUMBER_OF_MANAGEMENT_SESSIONS_PER_USER system flag). We recommend not reducing this setting. If you have a DMA supercluster with three Conference Manager clusters and a busy conferencing environment, we recommend increasing this value to 30.*

*The Automatic Password Generation feature, introduced in RMX version 7.0.2, is not compatible with the Polycom DMA system. On Polycom RMX MCUs to be used with the Polycom DMA system, disable this feature by setting the system flags NUMERIC_CONF_PASS_DEFAULT_LEN and NUMERIC_CHAIR_PASS_DEFAULT_LEN both to 0 (zero).*

*If the conference template selected for a conference specifies mixed AVC and SVC mode, the DMA system doesn't limit the choice of MCU to those that support mixed mode.*

*If the MCU selected doesn't support SVC at all, the DMA system starts the conference as an AVC-only conference. Otherwise, it starts a mixed mode conference.*

*If the MCU supports SVC-only conferences, but not the mixed AVC and SVC mode specified in the template, the conference simply doesn't start.*

*Use appropriately configured MCU pools and pool orders to limit mixed-mode conferences to MCUs that support mixed AVC and SVC mode.*

### RMX v7.7 Features Not Available in DMA System Templates

Version 7.7 of the RMX software introduced the following features that aren't available via standalone conference templates in this version of the DMA system:

- Customized Content Rate

  In an RMX profile, if this new option is selected, you can specify a custom content bit rate. To use this option via the DMA system, link the conference template to an RMX profile that implements the custom content bit rate you want to use.

  Alternatively, you can continue to use the existing Content Settings options (Graphics, Hi Res Graphics, and Live Video), which are available via the DMA system's standalone conference templates. These settings automatically determine an appropriate bit rate allocation for content.

- Mute participants except lecturer

  In an RMX profile, if this new Audio Settings option is selected and the conference is in lecture mode, all participants but the lecturer are muted. To use this option via the DMA system, link the conference template to an RMX profile that implements the option.

## Products Tested with This Release

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

*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 see the Current Interoperability Matrix.*

| Device | Version | Notes |
|---|---|---|
| Acme Packet Session Border Controller | | Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios. |
| Aethra X3 | 12.1.19 | |
| Aethra X7 | 12.1.7 | |
| Avaya 1000 series endpoints | | Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios. |
| Avaya Aura Communication Manager (H.323) | | Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios. |
| Avaya Aura Session Manager | | Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios. |
| Avaya Aura System Manager | | Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios. |
| Avaya One-X Communicator | | Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios. |
| BroadSoft BroadWorks Application Server | | Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios. |
| BroadSoft BroadWorks Media Server | | Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios. |
| BroadSoft BroadWorks Network Server | | Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios. |
| Cisco (Tandberg) 150 MXP | L6.1 | |
| Cisco (Tandberg) 1700 MXP | F9.1.2 | |
| Cisco (Tandberg) 6000 E Series | E5.3 | |
| Cisco (Tandberg) 6000 MXP | F9.1.2 | |
| Cisco (Tandberg) C20 | 5.1.3 | |
| Cisco (Tandberg) C40 | 5.1 | When the C40 is in H.323 mode, some compatibility issues exist when making point-to-point calls to SIP devices, including LifeSize Room 200 and Polycom HDX 4000. |

| Device | Version | Notes |
|---|---|---|
| Cisco (Tandberg) C90 | 5.1.3 | |
| Cisco (Tandberg) E20 | 4.1.1 | |
| Cisco (Tandberg) Edge95 MXP | F9.1.2 | |
| Cisco (Tandberg) EX90 | 5.1.3 | |
| Cisco (Tandberg) Gatekeeper | N6.1 | |
| Cisco (Tandberg) Gateway | G3.2 | |
| Cisco (Tandberg) MCU 4505 | 4.2 | |
| Cisco 3241 Gateway | 2.1 | |
| Cisco 3745 Gatekeeper | 12.4 | |
| Cisco IP Communicator | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco Unified Communication Manager | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco Unified IP Phones | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco Unified Personal Communicator | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco Unified Video Advantage | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco Unified Videoconferencing 5230 | | Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios. |
| Cisco VCS | X7.2 | |
| Edgewater EdgeMarc | | Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios. |
| IBM Sametime Connect Client | | Please consult the Polycom UC Deployment Guide for IBM Lotus Sametime Environments for a list of supported versions and interoperability scenarios. |
| IBM Sametime Media Manager Server | | Please consult the Polycom UC Deployment Guide for IBM Lotus Sametime Environments for a list of supported versions and interoperability scenarios. |
| LifeSize Desktop Client | 2.0.2.191 | |
| LifeSize Express 220 | 4.11.3 | |
| LifeSize Passport | 4.11.3 | |
| LifeSize Room | 4.7.21 | |

| Device | Version | Notes |
|---|---|---|
| LifeSize Team 200 | 4.7.21 | Some compatibility issues with other devices have been found, including these specific cases:<br>▪ When the Team 200 endpoint receives a call from a Lync or X-Lite software endpoint.<br>▪ When the Team 200 endpoint is in H.323 mode and makes a call to or receives a call from a SIP endpoint. |
| LifeSize Team 220 | 4.11.3 | |
| Microsoft Lync | | Please consult the Polycom UC Deployment Guide for Microsoft Environments for a list of supported versions and interoperability scenarios. |
| Polycom CMA | 6.2 | |
| Polycom CMAD | 5.2.3 | |
| Polycom DST Broad 5 | 2 | |
| Polycom DST K60 | 2.0.1 | |
| Polycom FX | 6.0.5 | |
| Polycom HDX | 3.1 | |
| Polycom m100 | 1.0 | |
| Polycom MGC 50+ | 9.0.4.3 | Can register with Call Server as free-standing MCU/gateway, but can't be added to Conference Manager's conferencing resource pool. |
| Polycom MGC Gateway | 9.0.4.3 | |
| Polycom PVX | 8.0.16 | |
| Polycom QDX4000 | 4.0.2 | |
| Polycom RealPresence Collaboration Server 800s | 8.0 | Supports mixed AVC and SVC conferences. |
| Polycom RealPresence Desktop | 2 | |
| Polycom RealPresence Group series | 4 | |
| Polycom RealPresence Mobile | 2 | |
| Polycom RealPresence Resource Manager | 7.1 | This version of the DMA system is not compatible with RealPresence Resource Manager v7.3. |
| Polycom RMX1000 | 2.1.2 | Can register with Call Server as free-standing MCU/gateway, but can't be added to Conference Manager's conferencing resource pool. |
| Polycom RMX1500, 2000, 4000 | 7.8 | Does not support mixed AVC and SVC conferences. |
| Polycom RSS4000 | 8.5 | |
| Polycom SoundPoint 601/650 SIP | 4.0.1 | |
| Polycom SoundStation IP4000 SIP | 3.1.7 | |
| Polycom Touch Controller Group series | 4 | |
| Polycom Touch Controller HDX | 1.6 | |
| Polycom VSX | 9.0.6.2 | |

| Device | Version | Notes |
|---|---|---|
| Polycom VVX1500 | 4.0.2 | Versions prior to 4.0.1 are not compatible due to a VVX defect. See DMA-6749 in the "Known Issues" list on page 28. |
| Radvision ECS Gatekeeper | 7.1.2.12 | |
| Radvision Scopia P10 Gateway | 5.7.2.0.25 | |
| Radvision Scopia XT1000 | 2.5.308 | |
| Radvision Scopia XT5000 | 3.0.122 | |
| Siemens OpenScape Desktop Client WE | | Please consult the Polycom UC Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications. |
| Siemens OpenScape Media Server | | Please consult the Polycom UC Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications. |
| Siemens OpenScape UC | | Please consult the Polycom UC Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications. |
| Siemens OpenScape Voice | | Please consult the Polycom UC Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications. |
| Siemens OpenStage Phone | | Please consult the Polycom UC Deployment Guide for the OpenScape Solution of Siemens Enterprise Communications. |
| Sony PCS-1 | 3.42 | |
| Sony PCS-G50 | 2.72 | |
| Sony PCS-TL50 | 2.42 | |
| Sony PCS-XG80 | 2.34 | |
| X-Lite software SIP phone | 5.0 | Some compatibly issues have been found when calling a Polycom HDX in SIP mode or a LifeSize Room200 in H.323 mode. |

## Open Source Software

The Polycom DMA system uses several open source software packages, including the CentOS operating system. The packages containing the source code and the licenses for this software are included on the Polycom DMA system software DVD in the /SRPMS directory.

The following table lists the open source software packages used in the Polycom DMA system, the applicable license for each, and the internet address where you can find it.

| Software Name | Version | License type | Address |
|---|---|---|---|
| Axis | 1.4.2 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| bsf | 2.3.0-rc1 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| CentOs | 5.8 | GPLv2 | https:/www.redhat.com/licenses/gpl.html |
| Cluster-glue | 1.0.5 | GPLv2 | http://www.gnu.org/licenses/old-licenses/gpl-2.0.html |
| commons-beanutils | 1.7 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |

| Software Name | Version | License type | Address |
|---|---|---|---|
| commons-collections | 3.2 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-configuration | 1.5 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-digester | 1.6 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-discovery | 0.2 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-fileupload | 1.2.1 | Apache License, Version 2 | http://commons.apache.org/fileupload/license.html |
| commons-httpclient | 3.0.1 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-io | 1.4 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-jexl | 1.0 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-jxpath | 1.2 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-lang | 2.3 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-logging | 1.0.4 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| commons-pool | 1.3 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| corosync | 1.2.5 | BSD | http://opensource.org/licenses/bsd-license.php |
| CXF | 2.2.3 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| dom4j | 1.5.2 | BSD-style | http://www.dom4j.org/license.html |
| drools | 4.0.0 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| generateDS | 2.7a | MIT license | http://www.opensource.org/licenses/mit-license.php |
| Guava-libraries | 13.0.1 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| Hibernate Annotations | 4.2.1.GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Hibernate (core) | 3.2.4 SP 1 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Hsqldb | 2.0.1-rc1 | BSD-style | http://hsqldb.org/web/hsqlLicense.html |
| JAF | 1.1 | Oracle Corporation Binary Code License Agreement | http://www.oracle.com/technetwork/java/javase/downloads/java-se-archive-license-1382604.html |
| jamon | 2.2 | BSD-style | http://jamonapi.sourceforge.net/#JAMonLicense |
| Java JRE | 1.7.0.9 | Oracle Corporation Binary Code License Agreement | http://www.java.com/en/download/license.jsp |
| JavaMail | 1.4 | Oracle Corporation Binary Code License Agreement | http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-eeplat-419426.html#javamail-1.4-oth-JPR |

| Software Name | Version | License type | Address |
|---|---|---|---|
| jaxb2 | 0.6.0 | BSD-style | http://confluence.highsource.org/display/J2B/License |
| JBOSS AS | 4.2.1 GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-aop | 1.5.5 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-cache | 1.4.1.sp14 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-jaxws | 2.0.0.GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-jmx | 4.2.1.GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-remoting | 2.2.2.sp1 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jboss-serialization | 4.2.1.GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| Jgroups | 2.4.8.GA | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| jcifs | 1.3.2 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| jna | 3.0.9 b0 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| joesnmp | 0.3.4 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| JSR 311 | 1.1.1 | CDDL-1.0 | http://www.opensource.org/licenses/cddl1.php |
| libesmtp | 1.0.4 | LGPLv2.1 | http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html |
| libnet | 1.1.4 | | |
| libxml2 | 1.2.3 | MIT License | http://www.opensource.org/licenses/mit-license.html |
| Log4j | 1.2.14 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| Neethi | 3.0.1 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| NSS | Part of Centos distribution | Mozilla Public License v1.1 | http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1 |
| NSS Tools | Part of Centos distribution | Mozilla Public License v1.1 | http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1 |
| NTP | Part of Centos distribution | Open Software License v3.0 | http://www.opensource.org/licenses/ntp-license.php |
| OpenDJ | 2.5.0 | CDDL-1.0 | http://www.opensource.org/licenses/cddl1.php |
| OpenFire | | Apache License, Version 2 | http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html |

| Software Name | Version | License type | Address |
|---|---|---|---|
| openSSH | Part of Centos distribution | OpenSSH | http://www.openssh.org |
| openSSL | Part of Centos distribution | OpenSSL | http://www.openssl.org/source/license.html |
| Postgresql91-server | 9.2.1 | PostgreSQL (similar to BSD or MIT) | http://opensource.org/licenses/postgresql |
| Postgresql91-contrib | 9.2.1 | PostgreSQL (similar to BSD or MIT) | http://opensource.org/licenses/postgresql |
| Postgresql91-libs | 9.2.1 | PostgreSQL (similar to BSD or MIT) | http://opensource.org/licenses/postgresql |
| Postgresql91 | 9.2.1 | PostgreSQL (similar to BSD or MIT) | http://opensource.org/licenses/postgresql |
| Postgresql91-devel | 9.2.1 | PostgreSQL (similar to BSD or MIT) | http://opensource.org/licenses/postgresql |
| Python | Part of Centos distribution | Python Software Foundation License Version 2 | http://python.org/download/releases/2.6.2/license |
| Quartz | 1.5.2 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| Rhino | | Mozilla Public License, v1.1 | http://www.mozilla.org/MPL/MPL-1.1.html<br>https://developer.mozilla.org/en/Rhino_License |
| sudo | 1.7.2p1 | ISCL | https://www.isc.org/software/license |
| Web App Solution, Inc. Flex 3 dashboard | | Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License, with a Creative Commons Plus License for commercial rights to the work. | http://creativecommons.org/licenses/by-nc-sa/3.0/<br>http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html |
| Xerces2 | See JBoss. | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| xmlschema | 2.0 | Apache License, Version 2 | http://www.apache.org/licenses/LICENSE-2.0 |
| The Open Source packages below are included in the Polycom DMA 7000 system as a consequence of being embedded in the Java Platform, Standard Edition Embedded, version 6.0. License text available at http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT | | | |
| 7-Zip | | Some files are LGPLv2.1; some have unRAR restriction; some are licensed under AES code license (see file) | |
| Ant | | Apache 2.0 | |
| Apache Derby | | Apache 2.0 | |
| Byte Code Engineering Library (BCEL) | v. 5 | Apache 1.1 | |

| Software Name | Version | License type | Address |
|---|---|---|---|
| Crimson | v1.1.1 | Apache 1.1 | |
| Cryptix | | Cryptix General License | |
| CS CodeViewer | v1.0 | BSD-like | |
| CUP Parser Generator for Java | v. 0.10k | (general permissive license) | |
| Document Object Model (DOM) | v. Level 3 | W3C SOFTWARE NOTICE AND LICENSE | |
| dom4j v. 1.6 | | BSD-like | |
| IAIK PKCS Wrapper | | BSD-like | |
| ICU4J | | ICU License | |
| Jing | | (general permissive) | |
| JLex: A Lexical Analyzer Generator for Java | v. 1.2.5 | (general permissive license) | |
| libpng official PNG reference library | | (general permissive license) | |
| Libungif – An uncompressed GIF library | | (general permissive license) | |
| LZMA Software Development Kit | | Common Public License (CPL) | |
| Mesa 3-D graphics library | v. 5 | The core Mesa library is licensed according to the terms of the XFree86 copyright (an MIT-style license). The Mesa source code is licensed under SGI FREE SOFTWARE LICENSE B (Version 1.1 [02/22/2000]) | |
| Mozilla Rhino | | Netscape Public License Version 1.1 | |
| NekoHTML | | Apache-like (1.1) | |
| NSIS | 1.0j | (see license file) | |
| Regexp Regular Expression Package | v. 1.2 | Apache 1.1 | |
| Regexp Regular Expression Package | v. 1.2 | Apache 1.1 | |

| Software Name | Version | License type | Address |
|---|---|---|---|
| RELAX NG Object Model/Parser | | MIT License | |
| RelaxNGCC | | (general permissive) | |
| RelaxNGCC | | version 2003-May-08 of the Info-ZIP copyright and license | ftp://ftp.info-zip.org/pub/infozip/license.html |
| Retroweaver | | (general permissive license) | |
| SAX | v. 2.0.1 | Public Domain | |
| Stax API | | BEA License (unique terms) | |
| Stripper | | BSD-like | |
| UPX | | GPL | |
| W3C XML Conformance Test Suites | v. 20020606 | W3C SOFTWARE NOTICE AND LICENSE | |
| W3C XML Schema Test Collection | v. 1.16.2 | W3C SOFTWARE NOTICE AND LICENSE | |
| W3C XML Schema Test Collection | | W3C DOCUMENT NOTICE AND LICENSE | |
| X Window System | | (general permissive license) | |
| Xalan J2 | | Apache 2.0 | |
| Xalan, Xerces | | Apache 1.1 | |
| XFree86-VidMode Extension | | Version 1.1 of Project Licence (BSD-like) | |
| XML Resolver Library | | Apache 2.0 | |
| XML Security | | Apache 1.1 | |
| Zlib | | (general permissive) | |

## Resolved Issues

The following table lists the issues resolved in the Polycom DMA 7000 system version 5.2.0 base release. See "What's New in the Version 5.2.2.4 Release" on page 4 for issues resolved in the subsequent maintenance releases.

| Issue ID | Found in Version | Description |
|---|---|---|
| DMA-9981 | 5.1 | After a rollback from 5.1 to 4.0.x followed by an upgrade to a later 4.0.x release, some configuration data was lost and the web server failed to start.<br>Note: This issue is also resolved in version 5.1.0 P1. |
| DMA-9882 | 5.1 | After a rollback from 5.1 to the previous version, configuration data was lost.<br>Note: This issue is also resolved in version 5.1.0 P1. |
| DMA-9875 | 5.0 | When an RMX MCU registered with the DMA system called Interactive Telepresence (ITP) endpoints, the calls failed.<br>Note: This issue is also resolved in version 5.0.2. |
| DMA-9792 | 5.0 | Registration issues with incorrectly named ITP endpoints caused multiple duplicate alerts. |
| DMA-9734 | 5.0.1 | The Dashboard on a DMA cluster incorrectly indicated that resource manager integration was disabled because it failed to check with all clusters in the supercluster. |
| DMA-9647 | 5.0.1, 5.1 | Unable to download CDR data when the system was accessed from a machine that had a GMT+ time setting (positive GMT offset). |
| DMA-9537 | 5.0.1 | The emergency purge script that runs when the disk is too full failed to delete old call signaling event audit records.<br>Note: This issue is also resolved in version 5.0.2. |
| DMA-7706 | 4.0.1 | In certain error-handling scenarios, the system sometimes leaked memory, threads, or resources. |

## Known Issues

The following table lists the known issues in this Polycom DMA 7000 system release.

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-11491 | 5.2 | When a point-to-point call traverses two clusters in the supercluster, the name of the originating and/or destination endpoint is incorrect or unresolved in the call history. | |
| DMA-10143 | 5.2 | When a two-server cluster is placed into maximum security mode, one of the servers remains in the previous security mode. | |
| DMA-10125 | 5.2 | Cascade links stay up for a long time after there are no more participants on the cascaded MCU. | |
| DMA-9992 | 4.0.2 | When a Cisco (Tandberg) EX90 endpoint using H.323 is in a call with an HDX endpoint using SIP, minor video artifacts may be seen on the Cisco endpoint. | |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-9991 | 4.0.1 | When a Cisco (Tandberg) MXP 6000 endpoint using H.323 calls an HDX endpoint using SIP, the Tandberg endpoint doesn't receive video. | |
| DMA-9971 | 5.0.1 | The DMA MIB couldn't be loaded into a Zenoss 3.2.1 network manager. | Download the MIB and in a text editor make the following changes in the IMPORTS section:<br>• Add these two lines:<br>TRAP-TYPE<br>FROM RFC-1215<br>• Change the line<br>::= { polycom 13 }<br>to<br>::= { enterprises 13885 }<br>Save the changes and load the modified file into the Zenoss 3.2.1 network manager. |
| DMA-9931, 10023, 10026 | 5.2 | MCU failover doesn't work for SVC calls or for AVC calls on RealPresence Collaboration Server 800s MCUs. | |
| DMA-9873 | 5.1 | Under rare circumstances, the DMA system may process an incomplete SIP message received over TCP and forward it to a downstream device. DMA hides the fact that the message is incomplete (its content is shorter than indicated in the Content-length header) by changing the Content-Length header to reflect the shortened content.<br>This happens when the DMA system receives an incomplete SIP message and the remaining part doesn't arrive within 2 seconds. It then terminates the TCP connection, but processes the incomplete message. | |
| DMA-9855 | 5.0.1, 5.1 | For reasons still being investigated, but probably related to DMA-7131, certain H.323 endpoints attempting to reach a VMR via a VBP are rejected as not registered. They believe they're registered and keep trying (sending ARQ), and the DMA keeps rejecting them (sending ARJ). This prevents the calls from completing, grows the database, and creates lots of network traffic. | |
| DMA-9854 | 5.1 | When a Cisco SX20 endpoint dialed into a VMR, it connected but didn't receive video. | The Cisco SX20 endpoint is not currently supported. |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-9775 | 5.1 | Call didn't connect dialing from Acme HDX h.323 to RPAD side VMR through h.323 trunk using 'id@ip' as dial string. | Add following script as preliminary for 'Resolve to conference room ID' dial rule: (change <*ip*> to external ip of your enterprise edge server):<br>if(DIAL_STRING.match( /[0-9]{4}@<*ip*>))<br>{<br>vmr = DIAL_STRING.replace(/([^@]*)@.*/i,"$1") ;<br>println(vmr);<br>DIAL_STRING=vmr;<br>} |
| DMA-9735 | 5.1, MFW 0.3.0 | Null pointer error when updating call properties for media streams. | |
| DMA-9708 | 5.0 | The default Request URI format option for the postliminary of a SIP peer is equivalent to the template:<br>#pscheme#:#oruser#@#phost#<br>The #pscheme# placeholder is the peer's scheme. This becomes "sips" if the peer's transport type is configured as TLS, even if the original Request URI's scheme was "sip."<br>Some SIP peers, such as the Cisco SBC, won't accept "sips" in the Request URI if other headers contain "sip."<br>The same problem will occur if any other format option that uses #pscheme# is selected. | To prevent such failures, do the following:<br>1. In the **Edit External SIP Peer** dialog box for the peer, go to the **Postliminary** tab.<br>2. Under **Request URI options**, change **Format** to **Free Form Template**.<br>3. In the **Template** field, replace #pscheme# with #orscheme# so that the Request URI template looks like this:<br>#orscheme#:#oruser#@#phost# |
| DMA-9700 | 5.1 | H.323 calls to an Aethra X7 endpoint using the DMA system as gatekeeper disconnect within one minute. | On the DMA system's **Call Server Settings** page, turn off **Terminate calls based upon failed responses to IRQs**. |
| DMA-9670 | 5.1 | SIP calls gatewayed by the DMA system to a RealPresence Access Director configured as an external H.323 gatekeeper fail because the gatekeeper doesn't have enough information to route the call. This happens because the LRQ that the DMA system sends to the gatekeeper contains only the E.164 digits, not the domain information, in destinationInfo. | On the DMA system's **Call Server Settings** page, turn on **For SIP calls gatewayed to an external gatekeeper, use the H.323 email ID as the destination instead of the E.164 number**.<br>**Note:** This option affects communications with all external H.323 gatekeepers to which the DMA system gateways SIP calls. |
| DMA-9579 | 5.1 | When calls to a VMR are rejected due to no capacity, in the conference history and CDR they aren't associated with the conference they tried to join. | To correctly associate such a call with the conference it attempted to join, match the call's destination string with the VMR number in the conference CDR. |
| DMA-9506 | 5.1 | When the USB Configuration Utility was used to configure a single-server system to use IPv6 only, the IPv6 network settings weren't properly implemented and the system didn't start. | |
| DMA-9496 | 5.1 | When the USB Configuration Utility was used to configure a single-server system to use IPv4+6 and split networking, the IPv6 signaling network settings weren't properly implemented. | |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-9463 | 5.1 | When an external endpoint's registration request is proxied to the DMA system by a RealPresence Access Director SBC, the DMA system incorrectly associates the endpoint with the "Internet/VPN" site instead of the site to which the RealPresence Access Director belongs. | |
| DMA-9361 | 5.0.1 | In a superclustered environment, some call events may appear out of order on the Call **Events** tab of the **Call Details** dialog box. | |
| DMA-9325 | 5.0 | On the **Call History** page, records found by a dial string search may have an empty **End Time** field even though they have an end time. | |
| DMA-9324 | 5.0 | When a rogue or neighbored call traverses two or more DMA clusters within one second, the call records from the clusters aren't always merged correctly, leading to inconsistent Call History information.<br>**Note:** This problem is resolved for callers managed by one of the clusters in the supercluster. | |
| DMA-9241 | 5.0 | Auto-negotiation is mandatory for 1000Base-T, but the DMA system allows it to be turned off. | Don't turn off auto-negotiation if you have a 1000Base-T network. |
| DMA-9139 | | The DMA system doesn't support CMA or RealPresence Resource Manager address book services for H.320 devices. | |
| DMA-9131 | | When a call forwarding loop involves an endpoint with multiple lines, the call keeps ringing that endpoint and can't be ended by the calling endpoint. | |
| DMA-9128 | 5.0 | The **Users** list can't be sorted on the **Associated Endpoints** column. | |
| DMA-9115 | 4.0.3 P1 | The DMA system creates an active call entry for an OCS chat INVITE. | |
| DMA-9098 | 4.0.3 | MCUs added to a DMA system prior to version 4.0 are deleted 30 days after upgrading to version 4.0 or later. | After upgrading, edit each MCU. In the **Edit MCU** dialog box, select **Permanent** to prevent the MCU's registration from expiring. |
| DMA-9085, 9088 | 5.0 | On the **Resource Management Server** page, **Model** is "CMA" for a RealPresence Resource Manager system. | |
| DMA-9027 | 4.0.3 | If SIP device authentication is enabled, it can be turned off for a specific endpoint, but not for a SIP peer. | |
| DMA-9010 | 5.0 | Sony PCS-1 and PCS-G50 endpoints are unable to remain connected in H.323 calls when they're registered to the DMA gatekeeper. | |
| DMA-8975 | 5.0 | Attempt to edit an MCU with active calls. The system displays an error message stating that it can't be deleted when there are active calls or conferences." | |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-8969 | 5.0.1 | On the **Call Info** tab of the **Call Details** dialog, the originator of the call may be misidentified. | The originator of the call is correctly identified on the **Call Events** tab of the **Call Details** dialog. |
| DMA-8952 | 5.0 | When multiple API clients are creating users, a concurrent sorted search can fail. | |
| DMA-8940 | 5.0 | The DMA system should drop a Bronze call if necessary to free up bandwidth for a Gold call. But if the calls are to the same VMR, it fails to do so. | |
| DMA-8936, 8937 | 5.0 | On point-to-point calls between Interactive Telepresence (ITP) systems, the ITP codecs (endpoints) may connect at different bit rates. | |
| DMA-8912 | 4.0.3 P1 | Under certain circumstances the status between local DMA clusters is incorrect even though the servers continue to function properly. | |
| DMA-8906 | 4.0.3 P1 | DMA UI allows host name and domain name entries of invalid length. | Limit host name and domain name to a combined maximum of 64 characters. |
| DMA-8904 | 5.0 | On dial-outs from a VMR, the system incorrectly records the originator of the call as the endpoint called (affects **Active Calls**, **Call History**, and CDRs). | |
| DMA-8885 | 5.0 | When a caller with a higher quality of service (QoS) setting dials into a conference and there isn't sufficient bandwidth, lower QoS calls are correctly dropped, but the higher QoS caller must redial in order to get into the conference. | |
| DMA-8875 | 5.0 | When a conference uses a custom template with auto layout enabled, auto layout sometimes doesn’t work. | |
| DMA-8869 | 5.0.1 | When a VMR call that traverses two DMA clusters and is pinned to the **Active Calls** list ends, its **Destination** field reverts from the MCU name to the dialed digits. | |
| DMA-8836 | 5.0 | Integrating the DMA system with a RealPresence Resource Manager doesn’t automatically integrate the RealPresence Resource Manager with the DMA system (that is, connect it to the DMA system’s API). | On the RealPresence Resource Manager, integrate it with the DMA system. The integration of the DMA system back to the RealPresence Resource Manager is automatically created. |
| DMA-8818 | 5.0 | At certain display resolutions and/or browser window sizes, some DMA dialog boxes may be cut off. | Use at least the minimum supported display resolution (1280x1024) and maximize the browser window. |
| DMA-8815 | 5.0 | When an RMX MCU is in dual stack (IPv4 + IPv6) mode, the DMA system attempts to respond to it via IPv6 even though it's in IPv4-only mode. | |
| DMA-8791 | 5.0 | When an RMX MCU registers with Call Server, its internal 172 address may appear in the list of media IP addresses. | The DMA system receives this IP address from the RMX MCU and simply reports it. |
| DMA-8715 | 5.0 | Removing a cluster from the supercluster may cause Adobe Flash to crash. | In a new browser window, log back in. |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-8675 | 5.0 | On calls to VMR, DMA system shows different requested and final bit rates than the MCU and endpoints show. | |
| DMA-8601 | 5.0 | Downloading call detail records (CDRs) can take a long time (> 2 minutes) when there are many CDRs in the system. | |
| DMA-8578 | 5.0 | When the DMA system and an RMX MCU were both in maximum security mode and the RMX MCU was registered with the DMA gatekeeper, the MCU couldn't securely connect to the DMA system. | |
| DMA-8567 | 5.0 | After switching from IPv4+IPv6 to IPv4 only, it may not be possible to download logs. | Reboot the system and try again. |
| DMA-8542 | 5.0 | After upgrading a two-server cluster to 5.0, the Dashboard may show one of the servers not available. | Reboot the unavailable server. |
| DMA-8514 | 5.0 | **Active Calls** and **Call History** may show different bit rates for same call. | |
| DMA-8489 | 5.0 | Under certain conditions, the host portion of an endpoint's SIP URI may be altered by the internal DMA call flow processing, and the call history record contains the altered host. | |
| DMA-8186 | 4.0.3 | Calls from the 32-bit version of the Lync 2010 client to a DMA VMR hosted on an RMX 1500 MCU don't receive video. | Use an RMX 2000 or 4000 MCU, or upgrade the user to the 64-bit version of Lync 2010. |
| DMA-7981 | 5.0 | In the call CDRs of VMR calls, the userRole field for participants is often null. | |
| DMA-7834 | 4.0, 4.0.3 | In rare instances, an upgrade or rollback can result in not being able to log in to the GUI as any user. | Reboot the DMA. |
| DMA-7829 | 4.0.3 | Integration to Microsoft Active Directory server sometimes fails with the message "Cache loading failed" and an alert icon with hovertext "Loading of the cache failed. Error: Timed out waiting for data from the directory."<br>This indicates that the AD server has insufficient performance. It may occur intermittently if the DMA is configured to use a DNS hostname or FQDN that aliases multiple AD servers, some of which have sufficient performance, and some of which do not. | Retry the integration until it succeeds.<br>To avoid this form of cache loading failure, integrate to an AD server that has sufficient performance. |
| DMA-7636 | 3.0 P1, 4.0, 4.0.1, 4.0.2 | M100 software endpoint version 1.0 cannot successfully make calls to or receive calls from Lync users through DMA when DMA/Lync integration is enabled. | |
| DMA-7614 | 4.0.2 | When conference management has failed over to the backup cluster for a territory, and the primary cluster is brought back online, there is a period of time (approximately 1 second for every 3000 enterprise users) when new calls can't join conferences in the territory. | |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-7541 | 4.0.2 | Deleting the territory used for Active Directory integration is incorrectly permitted. | If you need to delete the default territory, create a new territory and associate it with the AD integration prior to deleting the territory associated with AD integration. |
| DMA-7223, DMA-7230 | 4.0.2 | Due to a limitation of the Microsoft Lync client on Apple computers, video is not supported on calls to or from Lync clients for the Macintosh. | Voice-only calls are supported, as long as the endpoints involved support the G.711 codec. |
| DMA-7168 | 4.0.1 | HDX or Lync SIP calls to encrypted virtual meeting rooms (VMRs) via a virtual entry queue (VEQ) are hooked when being transferred to the VMR. | Use an unencrypted VMR. |
| DMA-7131 | 4.0.1 | A VBP allows endpoints on external networks to register through it to a LAN-side GK (DMA), proxying H.323 events from the public network to the internal network. The VBP sends all H.323 traffic from the same call signaling address and endpoint identifier (it uses the endpoint identifier of the last endpoint that successfully registered to the gatekeeper to refresh all its endpoint registrations).<br>As a result, DMA displays all VBP calls as having the same endpoint information as the device that sent the successful registration to the DMA and was assigned the endpoint identifier in the RCF. | |
| DMA-6644 | 4.0 | As required by the H.323 specification, the DMA system treats dial strings of the form "h323:<user>@<domain>" as url-IDs (H.323 Annex O) and dial strings of the form "<user>@<domain>" as email-IDs.<br>Other gatekeepers, such as CMA and VCS, treat dial strings of the form "<user>@<domain>" as url-IDs.<br>The DMA system's different treatment of these dial strings means that calls to non-neighbored external gatekeepers are likely to fail.<br>For compatibility purposes, the DMA should have a configuration option to treat these dial strings as url-IDs. | To configure the DMA system to behave like other gatekeepers,. edit the "Dial external networks by H.323 URL, Email ID, or SIP URI" dial rule, adding the following preliminary script:<br>DIAL_STRING=DIAL_STRING.replace(/^([^:@]*)@([^@]*)/,"h323:$1@$2"); |
| DMA-6524, 8447, 8500 | 4.0 | FECC (far end camera control) is not supported though the H323<->SIP gateway. The DMA system's protocol gateway supports only audio and video. | |
| DMA-6494 | 4.0 | When a Cisco endpoint registered to the DMA system has TLS verification enabled, encrypted calls to the endpoint fail. | On the endpoint, turn off TLS verification. |
| DMA-6482 | 4.0 | If the DMA system has a large number (over 100,000) of calls in its call history, upgrading to v4.0 can take over one hour. | In advance of the upgrade, on the History Retention Settings page, reduce the number of call history records to retain. |
| DMA-6480 | 4.0 | In a SIP to H.323 or H.323 to SIP call with content through the DMA system’s gateway, neither endpoint receives content-related statistics. | |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA-6459 | 4.0 | A conference passcode created on the DMA system may not conform to the passcode rules enforced by the MCU hosting the conference, causing calls to fail. | Make sure that the passcodes created on the DMA system meet the requirements of the MCUs that the system uses. |
| DMA-6103 | 3.0 | In an environment with both a DMA system and a Cisco Unified Conference Manager (CUCM), video path problems were encountered if certain endpoints (Cisco 9971, Polycom HDX9002, and Polycom V500) were registered to the CUCM. | Register the endpoints to the DMA system. |
| DMA-6101 | 4.0 | Under some circumstances, it may become impossible to log into one server of a two-server cluster because of a heartbeat failure stemming from a time disparity between the two servers. | Use NTP to synchronize the time on both servers and reboot the servers. |
| DMA-6033 | 4.0 | On the Conference Settings page, the DMA system's default maximum bit rate setting defaults to 2048, and that limit applies to both conference and non-conference (Call Server) calls. This may cause calls to or from Immersive Telepresence (ITP) systems requiring higher bit rates to fail. | On the Conference Settings page, change the default maximum bit rate setting to Unlimited. |
| DMA- 5862 | 3.0 | HDX endpoints expect H.323 bandwidth to be reserved in 64 kbps increments, but the DMA system uses smaller increments. The DMA system may, for instance, allocate 498 kbps for a call, and the call will use that. But the endpoint displays 448 (64 * 7). | |
| DMA- 5337 | 3.0 | The DMA system doesn't properly handle SIP signaling from Polycom V-series endpoints with firmware prior to v. 9.0.6 (Feb 02, 2010). | Upgrade the endpoints to v. 9.0.6 or later. |
| DMA-5313 | 3.0 | The Property Changes tab of the Call Details dialog box sometimes contains entries with duplicate sequence numbers. | |
| DMA- 5069 | 3.0 | In a superclustered environment, slight time drifts between clusters may produce CDR records out of order or duplicated.<br>If NTP services are properly configured, the system self-corrects, but by then the CDR data is already committed to the database. | NTP services usually keep clocks synced to the second, but sub-second differences may exist in the CDR ordering. Be aware that event order may not be 100% accurate due to time differences.<br>No loss of functionality or data occurs as a result of this issue. |
| DMA- 4604 | 3.0 | Calling a SIP endpoint registered to a Broadsoft Network Server from a SIP endpoint registered to the DMA system may result in a calling loop. | |
| DMA- 3750 | 2.3, 3.0 | In a two-server cluster, under certain adverse system and/or network conditions on either server, the virtual address may move between servers when it shouldn't. This could result in the disconnection of both SIP calls and H.323 calls. | The system automatically recovers, so disconnected callers can dial back in a short time later (1 - 10 seconds). |

| Issue ID | Found in Version | Description | Workaround |
|---|---|---|---|
| DMA- 3745 | 2.3 | It's possible to log into Server 1 of a two-server cluster and initiate an upgrade while Server 2 is still booting, causing the two servers to be out of sync and running different versions. | Do not perform upgrade, rollback, or system reconfiguration operations without both servers being up and active. |
| DMA- 3426 | 2.3, 3.0 | If a DMA cluster is the primary or backup for a territory, it can't be removed from the supercluster via the management interface until the territory responsibilities are removed. But there is no warning that territory responsibilities need to be corrected afterward. | After removing a cluster from a supercluster, always check and correct territory responsibilities. |
| DMA- 3390 | 2.3 | If a DMA cluster is the primary or backup for a territory, it could be removed from the supercluster via the USB Configuration Utility with no warning that territory responsibilities need to be corrected afterward. | After removing a cluster from a supercluster, always check and correct territory responsibilities. |
| DMA- 2797 | 2.3 | Some Sony endpoints that register with the DMA system become unregistered after five minutes. | |
| DMA- 2717 | 2.2 | If a "spoke" MCU with a cascade link to the "hub" MCU is registered with an unavailable GK, callers on the two MCUs are isolated from each other. No indication in GUI or logs. | Do one of the following:<br>Disable cascading for the conference while the GK is unavailable.<br>Register the RMX to a working GK.<br>Busy out the RMX while its GK is unavailable. |
| DMA- 2411 | 2.2 | Calls from endpoints registered to a Tandberg VCS GK don't include the IP address of the endpoint, so the DMA system can't determine the site to which the endpoint belongs. For cascaded conferences, the call ends up either in the hub conference or, if the VCS GK is in a defined site, in a spoke conference near the VCS GK. | Place the IP address of the VCS into a site near the bridges to be used for spokes. |
| DMA- 2362 | 2.3 | In some situations, SIP calls from an RMX to an HDX join with only video - no audio. | |
| DMA-2109 | 2.3 | Polycom V500 endpoints don't support failover of SIP registrations. | |
| DMA- 2014 | 2.3 | Polycom HDX and PVX endpoints don't support failover of SIP registrations. | |
| DMA- 1939, 1941, 1948 | 2.3 | H.323 calls using dial strings of the form <IP Address>##<Alias> sometimes fail. | The DMA supports such dial strings for both inbound and outbound calls, routing them to the specified gatekeeper or MCU IP address. Interpretation of the alias depends on the destination gatekeeper or MCU.<br>Use of this feature is not recommended, however, because support for it varies significantly among different kinds of endpoints. |

## Where to Get the Latest Product Information

To view the latest Polycom product documentation, visit the Support section of the Polycom website at www.polycom.com/support.

**Welcome to Polycom® Distributed Media Application™ (DMA™) 7000**
**(Software Version 5.2.0)**

## END USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE

IMPORTANT-READ CAREFULLY BEFORE USING THE SOFTWARE PRODUCT: This End-User License Agreement ("Agreement") is a legal agreement between you (and/or any company you represent) and either Polycom (Netherlands) B.V. (in Europe, Middle East, and Africa), Polycom Asia Pacific PTE Ltd. (in Asia Pacific), or Polycom, Inc. (in the rest of the world) (each referred to individually and collectively herein as “POLYCOM”), for the SOFTWARE PRODUCT (including any software updates or upgrades thereto) licensed by POLYCOM or its suppliers. The SOFTWARE PRODUCT includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By accepting these terms or by installing, downloading, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be and will be bound by the terms of this Agreement as a condition of your license. If you do not agree to the terms of this Agreement, your use is prohibited and you may not install or use the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed (not sold) to you, and its use is subject to the terms of this Agreement. This is NOT a sale contract.

1. GRANT OF LICENSE. Subject to the terms of this Agreement, POLYCOM grants to you a non-exclusive, non-transferable (except as set forth herein), revocable license to install and use the SOFTWARE PRODUCT solely on the POLYCOM product with which this SOFTWARE PRODUCT is supplied (the "PRODUCT"). You may use the SOFTWARE PRODUCT only in connection with the use of the PRODUCT subject to the following terms and the proprietary notices, labels or marks on the SOFTWARE PRODUCT or media upon which the SOFTWARE PRODUCT is provided. You are not permitted to lease, rent, distribute, assign, sell or sublicense the SOFTWARE PRODUCT, in whole or in part, or to use the SOFTWARE PRODUCT in a time-sharing, subscription service, hosting or outsourcing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the SOFTWARE PRODUCT (source code). Except as expressly provided below, this License Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights in respect to the SOFTWARE PRODUCT. You are solely responsible for use of the PRODUCT and the SOFTWARE PRODUCT by your agents, contractors, outsourcers, customers and suppliers and their compliance with this Agreement.

2. OTHER RIGHTS AND LIMITATIONS.

2.1 Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, modify or disassemble the SOFTWARE PRODUCT or otherwise reduce the SOFTWARE PRODUCT to human-perceivable form in whole or in part, except and only to the extent that such activity is expressly permitted by a third party license or applicable laws. The foregoing includes but is not limited to review of data structures or similar materials produced by SOFTWARE PRODUCT. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT. You may not use the SOFTWARE PRODUCT for any illegal purpose or conduct.

2.2 Back-up. Except as expressly provided for under this Agreement you may not copy the SOFTWARE PRODUCT; except, however, you may keep one copy of the SOFTWARE PRODUCT and, if applicable, one copy of any previous version, for back-up purposes, only to be used in the event of failure of the original. All copies of the SOFTWARE PRODUCT must be marked with the proprietary notices provided on the original SOFTWARE PRODUCT. You may not reproduce the supporting documentation accompanying the SOFTWARE PRODUCT.

2.3 No Modifications. You may not modify, translate or create derivative works of the SOFTWARE PRODUCT.

2.4 Proprietary Notices. You may not remove or obscure any proprietary notices, identification, label or trademarks on or in the SOFTWARE PRODUCT or the supporting documentation.

2.5 Software Transfer. You may permanently transfer all of your rights under this Agreement solely in connection with transfer of the PRODUCT, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades or updates, this Agreement, and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade or update, any transfer must include all prior versions of the SOFTWARE PRODUCT. However, if the SOFTWARE PRODUCT is marked "Not for Resale" or "NFR", you may not resell it or otherwise transfer it for value.

2.6 Copyright. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, programs and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by POLYCOM or its suppliers. Title, ownership rights, and intellectual property rights in the SOFTWARE PRODUCT shall remain in POLYCOM or its suppliers. Title and related rights in the content accessed through the SOFTWARE PRODUCT is the property of such content owner and may be protected by applicable law. This Agreement gives you no rights in such content.

2.7 Confidentiality. The SOFTWARE PRODUCT contains valuable proprietary information and trade secrets of POLYCOM and its suppliers that remain the property of POLYCOM. You shall protect the confidentiality of, and avoid disclosure and unauthorized use of, the SOFTWARE PRODUCT.

2.8 Dual-Media Software. You may receive the SOFTWARE PRODUCT in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single PRODUCT. You may not use or install the other medium on another PRODUCT.

2.9 Reservation of Rights. POLYCOM and its suppliers reserve all rights in the SOFTWARE PRODUCT not expressly granted to you in this Agreement.

2.10 Additional Obligations. You are responsible for all equipment and any third party fees (such as carrier charges, internet fees, or provider or airtime charges) necessary to access the SOFTWARE PRODUCT.

2.11 Additional Software. You may not install, access, or use any software on the PRODUCT unless such software was provided by or otherwise authorized by POLYCOM. POLYCOM may, in its sole discretion and in accordance with this Agreement or other applicable licenses, allow you to download and install certain support software on the PRODUCT, such as anti-virus software.

2.12 Benchmark Tests. You may not publish the results of any benchmark tests run on the PRODUCT, SOFTWARE PRODUCT, or any component of the SOFTWARE PRODUCT without written permission from Polycom.

2.13 Additional Features. POLYCOM may offer additional software features for its PRODUCTS. Use of these additional software features may require the purchase of a license. You may not install, access, or use any additional software features on PRODUCTS other than those listed on your license and only then once the proper number of licenses have been purchased and authorized by POLYCOM. You may use additional software features in a PRODUCT for trial purposes for a maximum of 30 days without purchasing a license.

3. SUPPORT SERVICES. POLYCOM may provide you with support services related to the SOFTWARE PRODUCT ("SUPPORT SERVICES "). Use of SUPPORT SERVICES is governed by the POLYCOM policies and programs described in the POLYCOM-provided materials. Any supplemental software code provided to you as part of the SUPPORT SERVICES is considered part of the SOFTWARE PRODUCT and is subject to the terms and conditions of this Agreement. With respect to technical information you provide to POLYCOM as part of the SUPPORT SERVICES, POLYCOM may use such information for its business purposes, including for product support and development. POLYCOM will not utilize such technical information in a form that personally identifies you.

4. TERMINATION. This Agreement will terminate automatically if you fail to comply with any of the terms and conditions of this Agreement. Polycom shall have the right to audit your use of the SOFTWARE PRODUCT in conjunction with this Agreement, and you will provide reasonable assistance for this purpose. In the event of any termination, you must cease use of the SOFTWARE PRODUCT, and destroy all copies of the SOFTWARE PRODUCT and all of its component parts. You may terminate this Agreement at any time by destroying the SOFTWARE PRODUCT and all of its component parts. Termination of this Agreement shall not prevent POLYCOM or its suppliers from claiming any further damages. If you do not comply with any of the above restrictions, this license will terminate and you will be liable to POLYCOM and its suppliers for damages or losses caused by your non-compliance. The waiver by POLYCOM of a specific breach or default shall not constitute the waiver of any subsequent breach or default.

5. UPGRADES. If the SOFTWARE PRODUCT is labeled as an upgrade or update, you must be properly licensed to use the software identified by POLYCOM as being eligible for the upgrade or update in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade or update replaces and/or supplements the software that formed the basis for your eligibility for the upgrade or update. You may use the resulting upgraded/updated SOFTWARE PRODUCT only in accordance with the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade or update of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single SOFTWARE PRODUCT package and may not be separated for

use on more than one PRODUCT. You shall maintain the SOFTWARE PRODUCT replaced by the upgrade or update solely for use as an archival copy for recovery purposes for the updated PRODUCT.

6. WARRANTY AND WARRANTY EXCLUSIONS.

6.1 Limited Warranty. Except as otherwise set forth in a Third Party License or in third party license terms set forth below, POLYCOM warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of shipment by POLYCOM, and (b) any SUPPORT SERVICES provided by POLYCOM shall be substantially as described in applicable written materials provided to you by POLYCOM. This warranty is valid only for the original purchaser. POLYCOM DOES NOT WARRANT THAT YOUR USE OF THE SOFTWARE PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT ALL DEFECTS IN THE SOFTWARE PRODUCT WILL BE CORRECTED. YOU ASSUME FULL RESPONSIBILITY FOR THE SELECTION OF THE SOFTWARE PRODUCT TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM THE SOFTWARE PRODUCT. POLYCOM'S SOLE OBLIGATION UNDER THIS EXPRESS WARRANTY SHALL BE, AT POLYCOM'S OPTION AND EXPENSE, TO REFUND THE PURCHASE PRICE PAID BY YOU FOR ANY DEFECTIVE SOFTWARE PRODUCT WHICH IS RETURNED TO POLYCOM WITH A COPY OF YOUR RECEIPT, OR TO REPLACE ANY DEFECTIVE MEDIA WITH SOFTWARE WHICH SUBSTANTIALLY CONFORMS TO APPLICABLE POLYCOM PUBLISHED SPECIFICATIONS. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

6.2 Warranties Exclusive. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THE SOFTWARE PRODUCT. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM POLYCOM OR THROUGH OR FROM THE SOFTWARE PRODUCT SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

NEITHER POLYCOM NOR ITS SUPPLIERS SHALL BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE SOFTWARE PRODUCT DOES NOT EXIST OR WAS CAUSED BY YOUR OR ANY THIRD PARTY'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO MODIFY THE SOFTWARE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

7. LIMITATION OF LIABILITY. YOUR USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE SOFTWARE PRODUCT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION DAMAGES FOR LOSS OF BUSINESS PROFITS OR REVENUE; BUSINESS INTERRUPTION OR WORK STOPPAGE; COMPUTER FAILURE OR MALFUNCTION; LOSS OF BUSINESS INFORMATION, DATA OR DATA USE; LOSS OF GOODWILL; OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF POLYCOM OR ITS SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM'S SUPPLIERS BE LIABLE FOR ANY DIRECT DAMAGES WHATSOEVER ARISING OUT OF THE USE OR THE INABILITY TO USE THE SOFTWARE PRODUCT. IN ANY CASE, POLYCOM'S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S. $5.00. NOTWITHSTANDING THE TERMS OF THIS SECTION 7, IF YOU HAVE ENTERED INTO A POLYCOM SUPPORT SERVICES AGREEMENT, POLYCOM'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT.

8. INDEMNITY. You agree to indemnify and hold harmless POLYCOM and its subsidiaries, affiliates, officers, agents, co-branders, customers, suppliers or other partners, and employees, from any loss, claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of the SOFTWARE PRODUCT, your connection to the SOFTWARE PRODUCT, or your violation of the Terms.

9. DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety due to local law, they will be limited to the duration of the applicable warranty.

10. EXPORT CONTROLS. You acknowledge that the SOFTWARE PRODUCT may be subject to export restrictions of various countries. You shall fully comply with all applicable export license restrictions and requirements as well as with all laws and regulations relating to the importation of the SOFTWARE PRODUCT, in the United States and in any foreign jurisdiction in which the SOFTWARE PRODUCT is used. Without limiting the foregoing, the SOFTWARE PRODUCT may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) any country to which the U.S. has embargoed goods; (ii) any end user known, or having reason to be known, will utilize them in the design, development or production of nuclear, chemical or biological weapons; or (iii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the SOFTWARE PRODUCT, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this SOFTWARE PRODUCT outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained. You further acknowledge that the SOFTWARE PRODUCT may include technical data subject to export and re-export restrictions imposed by US law.

11. MISCELLANEOUS.

11.1 Governing Law. This Agreement shall be governed by the laws of the state of California as such laws are applied to agreements entered into and to be performed entirely within California between California residents, and by the laws of the United States, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods (1980) and the Uniform Computer Information Transactions Act (UCITA) are hereby excluded in their entirety from application to this Agreement.

11.2 Entire Agreement. This Agreement represents the complete agreement concerning the SOFTWARE PRODUCT and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

11.3 Contact. If you have any questions concerning this Agreement, or if you desire to contact POLYCOM for any reason, please contact the POLYCOM office serving your country.

11.4 U.S. Government Restricted Rights. The software and documentation provided by Polycom pursuant to this Agreement are “Commercial Items,” as the term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are licensed to United States Government end users (1) only as Commercial Items and (2) with only those rights as are granted to all other users pursuant to the terms of this Agreement.

11.5 High Risk Use. The SOFTWARE PRODUCT is not fault-tolerant and is not designed or Intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the SOFTWARE PRODUCT could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Use"). You are not licensed to, and you agree not to, use, distribute or sublicense the use of the SOFTWARE PRODUCT in, or in conjunction with, High Risk Use. High Risk Use is STRICTLY PROHIBITED. POLYCOM AND ITS SUPPLIERS EXPRESSLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK USE.

11.6 Third Party Software. The SOFTWARE PRODUCT may be distributed with software governed by licenses from third parties (“Third Party Software” and “Third Party License”). Any Third Party Software is licensed to you subject to the terms and conditions of the corresponding Third Party License, notwithstanding anything to the contrary in this Agreement. More information on Third Party Licenses included in the SOFTWARE PRODUCT can be found in the documentation for each PRODUCT. Polycom makes no representation or warranty concerning Third Party Software and shall have no obligation or liability with respect to Third Party Software. If the Third Party Licenses include licenses that provide for the availability of source code and the corresponding source code is not included with the PRODUCT, then check the documentation supplied with each PRODUCT to learn how to obtain such source code.

BY INSTALLING, COPYING, OR OTHERWISE USING THIS SOFTWARE PRODUCT YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.

6001 America Center Drive
PO Box 641390
San Jose, CA 95164
U.S.A.

**APPLICATION PROGRAMMING INTERFACES LICENSE AGREEMENT**

IMPORTANT-READ CAREFULLY BEFORE USING THE APPLICATION PROGRAMMING INTERFACES: This Application Programming Interfaces License Agreement ("Agreement") is a legal agreement between you and/or any company you represent ("Licensee") and either Polycom (Netherlands) B.V. (in Europe, Middle East, and Africa), Polycom Asia Pacific PTE Ltd. (in Asia Pacific), or Polycom, Inc. (in the rest of the world) (each referred to individually and collectively herein as "POLYCOM"), for the API licensed by POLYCOM and, if applicable, included with the SOFTWARE PRODUCT. By clicking "I AGREE" or by installing, downloading, copying, or otherwise using the API, you agree to be and will be bound by the terms of this Agreement as a condition of your license. If you do not agree to the terms of this Agreement, your use is prohibited and you may not install or use the API.

The API is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The API is licensed (not sold) to you, and its use is subject to the terms of this Agreement. This is NOT a sale contract.

1. DEFINITIONS.

1.1 "Application Programming Interfaces" or "API" means POLYCOM technology, which may include object code, software libraries, software tools, sample source code, published specifications and Documentation. API shall include any future, updated or otherwise modified version(s) thereof furnished by POLYCOM (in its sole discretion) to Licensee.

1.2 "Documentation" includes, but is not limited to programmer guides, CDs, manuals, materials, and information appropriate or necessary for use in connection with the API.

2. GRANT OF LICENSE. Subject to the terms of this Agreement, POLYCOM hereby grants Licensee a limited, non-exclusive, non-transferable, royaltyfree license (without the right to sublicense) to use the API solely for the purpose of Licensee's internal development efforts to develop applications to work in conjunction with the POLYCOM products referenced in the API and for which the API was provided. Licensee shall have no right to distribute, license (whether or not through multiple tiers) or otherwise transfer the API to any third party or incorporate the API in any software, product, or technology.

3. OTHER RIGHTS AND LIMITATIONS.

3.1 A license key may be required in order to enable and expose APIs on certain PRODUCTS. You may not use or attempt to use features of the POLYCOM Software that POLYCOM has not exposed or enabled for the purpose of utilizing the SDKs and related APIs.

3.2 Copies. Licensee may copy the API only as necessary to exercise its rights hereunder; provided, however that Licensee may also make one (1) copy for back-up purposes and any reproduction of the API must be marked with the proprietary notices provided on the original API.

3.3 No Reverse Engineering. Licensee shall have no rights to any source code for any of the software in the API, except for the explicit rights to use the source code as provided to Licensee hereunder. Licensee may not reverse engineer, decompile, modify or disassemble the API or otherwise reduce the API to human-perceivable form in whole or in part, except and only to the extent that such activity is expressly permitted by this Agreement or applicable laws.

3.4 Third Party Software. Licensee acknowledges that effective utilization of the API may require the use of a development tool, compiler and other software and technology of third parties ("Third Party Software"). Licensee is solely responsible for procuring such Third Party Software and technology and the necessary licenses for the use thereof. POLYCOM makes no representation or warranty concerning Third Party Software and shall have no obligation or liability with respect to Third Party Software.

3.5 U.S Government Restricted Rights. The software and documentation provided by POLYCOM pursuant to this Agreement are "Commercial Items," as the term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are licensed to United States Government end users (1) only as Commercial Items and (2) with only those rights as are granted to all

other users pursuant to the terms of this Agreement.

3.6 No right is granted to Licensee to sublicense its rights hereunder. All rights not expressly granted are reserved by POLYCOM and, except as expressly set forth herein, no license is granted by POLYCOM under this Agreement directly, by implication, estoppel or otherwise, under any patent, copyright, trade secret or trademark or other intellectual property right of POLYCOM. Nothing herein shall be deemed to authorize Licensee to use POLYCOM's trademarks or trade names in Licensee's advertising, marketing, promotional, sales or related materials. POLYCOM reserves all rights not otherwise expressly granted in this Agreement.

3.7 Nonassertion By Licensee. Licensee agrees not to assert any patent rights related to the API or applications developed using the API against POLYCOM, POLYCOM's distributors, POLYCOM customers, or other licensees of the API for making, using, selling, offering for sale, or importing any products or technology developed using the API.

3.8 Benchmark Tests. You may not publish the results of any benchmark tests run on the API without written permission from Polycom.

4. OWNERSHIP. As between POLYCOM and Licensee, POLYCOM or its licensors shall own and retain all proprietary rights, including all patent, copyright, trade secret, trademark and other intellectual property rights, in and to the API and any corrections, bug fixes, enhancements, updates, improvements, or modifications thereto and Licensee hereby irrevocably transfers, conveys and assigns to POLYCOM all of its right, title, and interest therein. POLYCOM shall have the exclusive right to apply for or register any patents, mask work rights, copyrights, and such other proprietary protections with respect thereto. Licensee acknowledges that the license granted under this Agreement does not provide Licensee with title or ownership to the API, but only a right of limited use under the terms and conditions of this Agreement.

5. SUPPORT. POLYCOM will not provide any support for the API under this Agreement. Nothing herein shall be construed to require POLYCOM to provide support services or updates, upgrades, bug fixes or modifications to the API.

6. CONFIDENTIALITY.

6.1 The API contains valuable proprietary information and trade secrets of POLYCOM and its suppliers that remain the property of POLYCOM. You shall protect the confidentiality of, and avoid disclosure and unauthorized use of, the API.

6.2 Licensee shall not disclose, advertise, or publish the terms and conditions of this Agreement without the prior written consent of POLYCOM. Any press release or publication regarding this Agreement is subject to prior review and written approval of POLYCOM.

7. HEALTHCARE APPLICATIONS SUITABILITY. LICENSEE SHALL BE SOLELY RESPONSIBLE FOR ANY PRODUCT USE OR APPLICATION DEVELOPED USING POLYCOM'S API THAT MAY FALL UNDER UNITED STATES FOOD AND DRUG ADMINISTRATION REGULATION, OR OTHER SUCH SIMILAR REGULATORY JURISDICTION, INCLUDING ANY AND ALL RESPONSIBILITY FOR COMPLIANCE TO SUCH REGULATION AS MAY BE APPLICABLE. LICENSEE ACKNOWLEDGES THAT POLYCOM PROVIDES THE API AS A GENERAL PURPOSE DEVELOPMENT TOOL TO LICENSEE.

8. NO WARRANTY. The API and Documentation are provided "AS-IS" without any warranty whatsoever. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM POLYCOM OR THROUGH OR FROM THE API SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. POLYCOM DOES NOT WARRANT THAT THE API AND DOCUMENTATION ARE SUITABLE FOR LICENSEE'S USE, THAT THE API OR DOCUMENTATION ARE WITHOUT DEFECT OR ERROR, THAT OPERATION WILL BE UNINTERRUPRED, OR THAT DEFECTS WILL BE CORRECTED. FURTHER, POLYCOM
MAKES NO WARRANTY REGARDING THE RESULTS OF THE USE OF THE API AND DOCUMENTATION.

9. LIMITATION OF LIABILITY. YOUR USE OF THE API IS AT YOUR SOLE RISK. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE API. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION DAMAGES FOR LOSS OF

BUSINESS PROFITS OR REVENUE; BUSINESS INTERRUPTION OR WORK STOPPAGE; COMPUTER FAILURE OR MALFUNCTION; LOSS OF BUSINESS INFORMATION, DATA OR DATA USE; LOSS OF GOODWILL; OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE API OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF POLYCOM OR ITS SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM'S SUPPLIERS BE LIABLE FOR ANY DIRECT DAMAGES WHATSOEVER ARISING OUT OF THE USE OR THE INABILITY TO USE THE API. IN ANY CASE, POLYCOM'S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE API OR U.S. $5.00.

10. INDEMNITY. You agree to indemnify and hold harmless POLYCOM and its subsidiaries, affiliates, officers, agents, co-branders, customers, suppliers or other partners, and employees, from any loss, claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of the API, your connection to the API, or your violation of the Terms.

11. DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety due to local law, they will be limited to the duration of the applicable warranty.

12. TERM AND TERMINATION.
12.1 This Agreement will terminate automatically if you fail to comply with any of the terms and conditions of this Agreement and you will be liable to POLYCOM and its suppliers for damages or losses caused by your non-compliance. The waiver by POLYCOM of a specific breach or default shall not constitute the waiver of any subsequent breach or default.
12.2 Either party shall have the right to terminate the Agreement, upon thirty (30) days written notice to the other party.

12.3 Upon termination of this Agreement, Licensee will immediately cease using the API Development Kit, and Licensee agrees to destroy all adaptations or copies of the API and Documentation, or return them POLYCOM upon termination of this License.
12.4 Polycom shall have the right to audit your use of the API in conjunction with this Agreement, and you will provide reasonable assistance for this purpose.

12.5 The rights of Polycom and your obligations contained in this Agreement survive any expiration or termination of this Agreement.

13. MISCELLANEOUS.
13.1 ASSIGNMENT. Licensee may not assign this Agreement or any interest or rights granted hereunder to any third party without the prior written consent of POLYCOM. A change of control or reorganization of Licensee pursuant to a merger, sale of assets or stock shall be deemed to be an assignment under this Agreement. This Agreement shall terminate immediately upon occurrence of any prohibited assignment.

13.2 EXPORT CONTROLS. You acknowledge that the API may be subject to export restrictions of various countries. You shall fully comply with all applicable export license restrictions and requirements as well as with all laws and regulations relating to the importation of the API, in the United States and in any foreign jurisdiction in which the API is used. Without limiting the foregoing, the API may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) any country to which the U.S. has embargoed goods; (ii) any end user known, or having reason to be known, will utilize them in the design, development or production of nuclear, chemical or biological weapons; or (iii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the API, you are agreeing to the foregoing and you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this API outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained. You further acknowledge that the API may include technical data subject to export and re-export restrictions imposed by US law.
13.3 WAIVER. No failure by either party to exercise or enforce any of its rights under this Agreement will act as a waiver of such rights and no waiver of a breach in a particular situation shall be held to be a waiver of any other or subsequent breach.

13.4 SEVERABILITY. If any provision of this Agreement is found invalid or unenforceable, that provision will be enforced to the maximum extent possible and the other provisions of this Agreement will remain in force.

13.5 Governing Law. This Agreement shall be governed by the laws of the state of California as such laws are

applied to agreements entered into and to be performed entirely within California between California residents, and by the laws of the United States, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods (1980) and the Uniform Computer Information Transactions Act (UCITA) are hereby excluded in their entirety from application to this Agreement.

13.6 Entire Agreement. This Agreement represents the complete agreement concerning the API and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

13.7 Contact. If you have any questions concerning this Agreement, or if you desire to contact POLYCOM for any reason, please contact the POLYCOM office serving your country.

BY INSTALLING, COPYING, OR OTHERWISE USING THE API YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.


4750 Willow Road
Pleasanton, CA 94588
U.S.A.

* * *



* * *



* * *

**ORACLE AMERICA, INC. LICENSE TERMS**

**Java Platform, Standard Edition Embedded, version 6.0**

1. Java Technology Restrictions. The end user licensee shall not create, modify, change the behavior of classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Oracle in any naming convention designation. In the event that the end user licensee creates an additional API(s) which: (a) extends the functionality of a Java Environment; and (b) is exposed to third party software developers for the purpose of developing additional software which invokes such additional API, the end user licensee must promptly publish broadly an accurate specification for such API for free use by all developers.
2. Trademarks and Logos. This License does not authorize an end user licensee to use any Oracle America, Inc. name, trademark, service mark, logo or icon. The end user licensee acknowledges that Oracle owns the Java trademark and all Java-related trademarks, logos and icons including the Coffee Cup and Duke ("Java Marks") and agrees to: (a) comply with the Java Trademark Guidelines at **http://www.oracle.com/html/3party.html**; (b) not do anything harmful to or inconsistent with Oracle's rights in the Java Marks; and (c) assist Oracle in protecting those rights, including assigning to Oracle any rights acquired by Licensee in any Java Mark.
3. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of your license. Source code may not be redistributed unless expressly provided for in the terms of your license.
4. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file, available at this link: http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT