Release Notes

Polycom® Distributed Media Application™ 7000 System, Version 4.0.3 P4 Release

Polycom® announces the release of its Polycom® Distributed Media Application™ (DMA™) 7000 System, version 4.0.3 P4. This document provides the latest information about this release.

Topics

Copyright Information

3725-76300-001R4 (08/2012)

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 and the Call Server, 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 33.

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 and improves efficiency.
- Supports up to 64 MCUs. MCUs can be added on the fly without impacting end users and without requiring re-provisioning.
- Can be configured as a two-server cluster, providing a highly reliable system with no single point of failure.

Call Server

- Provides complete endpoint registration and call routing services for both H.323 and SIP protocols. It also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to begin transitioning to SIP in a gradual, orderly, and cost-effective manner.
- Provides bandwidth management, and can be integrated with a Juniper Networks Session and Resource Control Module (SRC) to provide bandwidth assurance services.
- Comes with a default dial plan that covers many common scenarios, but which can easily be modified.
- Can be deployed as a *supercluster* of up to five geographically dispersed, but centrally managed, Polycom 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 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.

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.

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 CMA 5000 system to obtain site topology and user-to-device association data.

Software Version History

Version	Release Date	Features
4.0.3_P4	August 2012	Maintenance release to fix specific issues.
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.
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.

What's New in the Version 4.0.3 P4 Release

The version 4.0.3 P4 release addresses some issues found since the previous version 4.0.3 releases and replaces those releases.

Issues Resolved in Versions 4.0.3 P1-P4

The following table lists the issues resolved in the 4.0.3 P1through P4 releases.

Issue ID	Description
DMA-3802	During a bridge failover in a Microsoft Lync environment, calls from Lync clients sometimes failed to automatically reconnect, and other SIP calls sometimes took several seconds longer than usual to reconnect. This issue is resolved by using RMX version 7.6.1.136 or newer.
DMA-6749	The SIP to H.323 GW dropped calls involving a VVX endpoint running a version prior to 4.0.1 because the VVX mishandled the IRQ/IRR (EBCS-14). Leaving the new option on the **Call Server Settings** page turned off prevents this problem (see "Feature Enhancements in Version 4.0.3 P1" on page 5).
DMA-7250	Under certain circumstances, there was a significant discrepancy between the number of endpoints with an active registration status on the Endpoints page and the number of active registrations reported on the Dashboard's Call Server Registrations pane.
DMA-7267	The DMA system starts the call history trail from the first moment a call is presented to the DMA. If an LRQ was received from a neighbored gatekeeper that has a call ID, DMA recorded the originating entity as the gatekeeper that sent the LRQ, rather than the call that initiated the ARQ or sent the call setup.

Issue ID	Description
DMA-7599	In previous releases, the DMA gatekeeper was removing all aliases for a particular endpoint upon receipt of a (Unregister Request) URQ rather than just the alias specified in the URQ. This negatively impacted DMA<->VBP interop, since the VBP aggregates all aliases as a single endpoint, and upon receipt of a single URQ, DMA would unregister all endpoints that were registering to the DMA through the VBP.
DMA-7812	For gateway calls between some endpoints, the video wasn't displayed on one of the endpoints.
DMA-7898	If the DMA system's connection to a Microsoft Exchange Server was dropped and its attempt to reconnect failed, the reconnection attempt never timed out and the system never retried. This caused PCO meeting requests not to be processed.
DMA-7941	Under certain conditions, a cluster could propagate some of its existing data to the supercluster it was attempting to join before its data was replaced with the supercluster's data. This could result in corrupt data records supercluster-wide. The data on the cluster attempting to join the supercluster is now removed before the join attempt instead of later in the process.
DMA-7961	When searching for users with some combinations of search parameters (especially when searching by conference rooms), not all search parameters were taken into account. As a result, users not matching the search criteria were returned or, when searching for a non-existent conference room, an "acess error" message appeared.
DMA-8078	Calls from Lync endpoints to a VMR were dropped after 30 minutes.
DMA-8085	Calls from Cisco (Tandberg) MXP endpoints to a Polycom RSS recording and streaming server via a DMA system failed if the DMA system was in routed mode.
DMA-8086	Incorrect path in upgrade script prevented a process from stopping, potentially affecting upgrade.
DMA-8089	Added a subnet name field (required) to make it easier to administer and identify subnets when there are many.
DMA-8102	DMA gatekeeper was not responding to LRQs.
DMA-8171	Integration with a Microsoft Active Directory containing multiple users in the same domain with the same user name caused AD integration to fail. This condition no longer causes AD integration to fail. But only one of the duplicate users is imported.
DMA-8190	Under load (1000-1200 concurrent H.323 calls) and in routed mode, a DMA cluster failed over to the backup cluster for the territory, resulting in dropped calls.
DMA-8198	Direct Dial VEQ calls failed if the target VMR contained 10 digits.
DMA-8269	If the DMA system contained multiple large backup files, the Backup and Restore page took an extremely long time to load, sometimes causing the user to be logged out before it finished.
DMA-8293	Certain Sony endpoints registered to the DMA gatekeeper were being disconnected by the gatekeeper because they didn't handle IRQ/IRR properly. Leaving the new option on the **Call Server Settings** page turned off prevents this problem (see "Feature Enhancements in Version 4.0.3 P1" on page 5).
DMA-8301	Microsoft OCS R2 clients were unable to connect to a DMA VMR when using numeric dialing.
DMA-8331	When a SIP endpoint called another endpoint in a different site via a network cloud, the call failed and the DMA system experienced an internal error.
DMA-8728	When upgrading to 4.0.3 P1, a database index rebuild problem resulted in corruption of data. Note: Customers experiencing this issue must roll back from 4.0.3 P1 to their previous version and then upgrade to 4.0.3 P3.

Issue ID	Description
DMA-8732, DMA-9168	Under certain circumstances (such as when a Lync endpoint is part of the call), an RMX MCU sends a large number of SIP INFO packets containing Media Control requests. This could lead to an excessively large audit database on the DMA system. To avoid this problem, the DMA system no longer records Media Control requests from RMX MCUs in its audit database file.
DMA-8796	When upgrading a system with a large number of users to 4.0.3 P1, the download of the very large upgrade log caused the Flash plugin to crash when the Software Upgrade page was opened.
DMA-8968	When ill-behaved endpoints flooded the DMA system with GRQ/RRQ messages, the hard disk became full. Now the system temporarily blacklists any such device (ignoring all signaling from it until it stops sending messages more frequently than the specification permits). If the device is or was registered, it's also quarantined, and it remains so until manually removed from quarantine. In addition, a new alert (5002) is triggered.
DMA-8979	The DMA system was failing to properly identify certain endpoints behind a VBP device because it only checked the version ID field. Now the system also checks the product ID field.
DMA-9069	When responding to a registration request with a registration reject (RRJ) message providing alternate gatekeeper information, the DMA system specified reason as undefined. Because of that, Tandberg endpoints ignored the alternate gatekeeper information and kept trying to register. Now the system specifies reason as resource unavailable, and Tandberg endpoints use the alternate gatekeeper information.
DMA-9071	When an enterprise user attempted to log into a DMA system, and the Active Directory server failed to respond to authenticate the user, the DMA system waited forever for a response, preventing even local users from logging in. Now the authentication attempt times out after about 140 seconds.
DMA-9084, DMA-9124	After a call from a site managed by the DMA system to the Internet/VPN site ended, the Site Link Statistics page continued to show its bandwidth in use.
DMA-9174	When it received an LRQ for a VMR from a neighbor, but there was no follow-up message and the call never completed, the DMA system nevertheless reported this as an active call.
DMA-9184	In some circumstances after the DMA system received a BRQ message requesting a bit rate change for a call, it displayed an incorrect bit rate for that call in the Active Calls list.
DMA-9204	Improper handling of expired registration removals caused new registrations to fail.
DMA-9218	Under some circumstances, when the system quarantined an inactive endpoint, it set the registration status to Quarantined instead of Quarantined Inactive. This caused the system to improperly handle a subsequent expired registration removal of that endpoint, triggering the problem described in DMA-9204.

Feature Enhancements in Version 4.0.3 P1

The Polycom DMA system version 4.0.3 P1 included the following feature enhancements and new functionality. For more information on these features, see the online help.

- New call server settings option

  Because some endpoints respond to an IRQ with an IRR indicating invalid call or containing no call information, it may not be desirable to let the DMA gatekeeper terminate calls in such circumstances. A new setting on the **Call Server Settings** page, **Terminate calls based on failed responses to IRQs**, makes that behavior optional. The setting defaults to off.

- Subnet naming

  To make site topology management easier when there are many subnets, a Name field has been added to the **Add Subnet** dialog box. Now, when adding a subnet to a site, the subnet must be given a unique name.

What's New in the Version 4.0.3 Release

The version 4.0.3 release is primarily a maintenance release that fixes a number of issues found in the version 4.0 base release or version 4.0.1 or 4.0.2 releases and replaces those releases. In addition, it includes the feature enhancements described below.

Feature Enhancements in Version 4.0.3

The Polycom DMA system version 4.0.3 includes the following feature enhancements and new functionality. For more information on these features, see the *Polycom DMA System Operations Guide* and the online help.

- Device authentication enhancements

  The Device Authentication page supports the following new functionality:

  - Inbound SIP device authentication using the SIP digest authentication mechanism (RFC 3261 and RFC 2617).
  - Outbound authentication with external SIP peers using the SIP digest authentication mechanism.

- Added functionality regarding external SIP peers

  This version of the Polycom DMA system adds the following external SIP peer configuration enhancements:

  - Support for SIP digest authentication, with options for handling both 401 and 407 responses.
  - Explicit settings for next hop address, destination network (domain), and adding a route header.
  - Ability to select from several preconfigured To header and Request-URI formats or specify custom formats.
  - Ability to specify Request-URI and optional other headers for outbound registration.
  - Explicit setting for stripping prefixes.

- Active Directory integration improvements

  The Microsoft Active Directory integration feature was modified to improve performance and scalability, significantly reducing the time needed to integrate to AD, re-synchronize with AD, and restart a server that's integrated with AD.

  The system now supports integrating with ADs containing up to 1,000,000 users and 1,000,000 groups. Up to 10,000 groups may be imported.

- Database performance improvements

  LDAP database performance was increased overall. This improves all LDAP-based operations, including bandwidth management, call rate, registration rate, supercluster operations (join, leave, and data replication), and AD integration.

- Ability to select multiple endpoints on Endpoints page

  Multi-select makes it possible to block, quarantine, or delete multiple devices at a time.

- Log forwarding

  This version of the Polycom DMA system can be configured to forward selected log entries to a central log management server.

- New predefined variable for registration policy scripts

  The new EP_VERSION variable (the endpoint software version number) makes it possible to test for version compliance in a registration policy script.

Issues Resolved in Version 4.0.3

The following table lists the issues resolved in this release.

Issue ID	Description
DMA-4756	Administrators had to delete inactive registrations one at a time. Now, administrators can select multiple inactive registrations and delete them all at once.
DMA-5946	The active call count on the Endpoints page was not being updated properly in all circumstances.
DMA-6076	Alert 3405 (CPU utilization > 50% and < 75%) was being triggered incorrectly. Enhanced CPU monitoring is now in place.
DMA-6188	DMA failed to report bandwidth limitations applied by the call admission control policy, which resulted in the bandwidth limitation not being honored.
DMA-6264	Point to point calls from DMA registered endpoints to Lync clients were failing.
DMA-6393	The call history detail for a call involving a Lync registered endpoint included no information for such an endpoint.
DMA-6451	When the system was configured to block endpoint registrations except for endpoints manually allowed by the administrator, a change to the signaling IP address or port of an allowed endpoint caused the endpoint to become blocked, even when the "Ignore IP and port changes" option was selected. The system now honors the "Ignore IP and port changes" option.
DMA-6560	Alert 3402 pertaining to the purging of old log files would always appear on some systems.
DMA-6954	CTS calls to DMA failed intermittently. Downspeed message passing caused issues.
DMA-7025	The start time for alert notifications was being overwritten with the end time when an alert was resolved.
DMA-7075	Endpoints screen refresh caused scroll location to be lost.
DMA-7101	UUID's are unhelpful in the UI and names should be used whenever possible.
DMA-7119	A brief outage in one of DMA's underlying services would cause the system to lose knowledge of its licensing.
DMA-7145	On boot-up until the internal DMA LDAP processes were fully functional and healthy, DMA did not start its primary services. This caused incorrect data on GUIs, replication of bad/corrupt data across a supercluster, and timing issues with HA-configured DMA servers that could lead to automatic reboots and loss of current calls on both servers (even if the active server is not the one being booted). It also sometimes caused DMA services to enter a partially active and partially inactive state for which a manual reboot (with the power switch) was the only remedy.
DMA-7169	Improved LDAP database performance.

Issue ID	Description
DMA-7173	In rare circumstances, one of DMA's underlying services restarted unexpectedly causing a brief outage in DMA.
DMA-7195	When a certificate failed to install, the appropriate error message wasn't displayed.
DMA-7198	If an endpoint's registration timed out and it later re-registered, the registration refresh timer would fail to register a second timeout, and the endpoint would be reported as Active in the DMA GUI despite being inactive.
DMA-7219	During the upgrade process, DMA creates a backup of the system configuration (this backup is restored during the rollback process). DMA now removes the backups from previous DMA versions that cannot be rolled back to.
DMA-7235	DMA did not properly parse certificates with spaces in the certificate's nickname.
DMA-7238	When the DMA received SIP message types that it doesn't support, it was possible for internal resources (memory and threads) to be leaked. Internal SIP stack and application message handling logic have been modified to not leak these resources anymore on reception of unsupported message types.
DMA-7239	If a DMA system was rolled back from v4.0.2 to the initial release of v2.3.0, the system was unable to register to an external gatekeeper.
DMA-7259	Improvement request: Add new registration policy script variable, EP_VERSION, that enables registration policy decisions based on the version field specified in a registration request packet sent from a device.
DMA-7276	High bit-rate calls with Internet/VPN site in media path failed because of improper bandwidth calculation.
DMA-7295	Any number dialed, including direct IP addresses, was being interpreted by prefix dialing rules. Now those rules ignore any dial string that is a properly formatted IP address. For example, before the fix, with a dialing prefix of 72 configured on the DMA these dial strings would resolve to the 72 prefix device: 72.34.56.34, 72.1.1.1##5678. Now the prefix dial resolution ignores these dial strings because they are IP addresses.
DMA-7298	Several issues existed where joining or leaving superclustering could fail or leave either the leaving/joining cluster in a bad state or leave the cluster being joined/left in a bad state. Work was done to make the supercluster administrative actions (join/leave) more robust and logic was implemented to auto-correct many of the issues if they still arise. Several boot-up and shutdown issues that could cause data loss when joining/leaving superclusters were also addressed. Emergency administrative actions for restarting supercluster services were also added to the DMA GUI screen in case auto-corrective measures fail.
DMA-7303	In 4.0.2, there was a requirement for Lync users to select "Share my video" to have the call complete successfully. That requirement is no longer in force. To eliminate this requirement, Lync calls are established using G.711 for voice. With this change, DMA can support audio only, G.711 calls to the Macintosh Lync client.
DMA-7321	Improvement request: Improve performance and scalability of Microsoft Active Directory integration.
DMA-7363	Some H.323 devices may send full Registration Request messages (RRQs) rather than Lightweight Registration Request messages (LWRRQ and RRQ with the isKeepAlive flag set to true) to refresh their gatekeeper registration. Prior to the 4.0.3 release, DMA would treat these full RRQ's as a new registration and write the endpoint configuration back to gatekeeper's registered endpoint database. This caused performance issues under registration load and during territory failover. In v4.0.3, RRQs received by the DMA gatekeeper are compared with the existing device registrations, and if the data from the RRQ message matches the existing endpoint registration, no change is made to the endpoint database.

Issue ID	Description
DMA-7365	In rare and emergency situations the DMA disk may become full, which may result in undefined general DMA behavior, loss of logging data, and loss of audit/CDR data. A feature has been added so that when DMA detects its disk is almost full, it institutes the following emergency space recovery procedures: 1) It removes all but the most recent backup file stored on the DMA. 2) If more space is still needed, it removes all archived logs stored on the DMA. If this occurs, it changes the current documented log and backup retention policy.
DMA-7371	Removed Alert 1005 because this is not (necessarily) an error condition.
DMA-7399	Unable to change logging frequency on systems that have been upgraded to v4.0.2.
DMA-7427	H.323 signaling messages could build up in memory without being processed into the audit database. Over time, this could lead to reduced system performance, and eventually a system restart would be required. These H323 signaling messages are now thrown out if they haven't been processed within a reasonable time period so that the overall system integrity doesn't become compromised.
DMA-7445	When viewing details for a registered endpoint, the territory name would not show up next to the Territory label.
DMA-7456	Gateway call (SIP->H323) failed if the dial string was an email ID.
DMA-7505	The DMA upgrade process could not decode all portions of ISDN Gateway configuration. The DTO record factory was unknown to daotool; therefore, when the upgrade attempted to listAll objects, MCUs (commobjects) that had GatewayProfiles couldn't be decoded and threw. This aborted the roundtrip and caused the data loss.
DMA-7542	Deleting a territory that a user was customized with led to PCO VMRs not having a territory properly assigned. Now when a territory is deleted, users assigned to it are reassigned to the default territory.
DMA-7543	When H.323 endpoints registered to an external GK, such as CMA, attempted to call Lync (an external SIP peer), the call failed.
DMA-7601	There are scenarios in which 2 H.460 clients behind a VBP cannot open an H.225 connection directly to each other (i.e., there may be a secondary NAT behind the primary NAT, etc.); therefore, DMA must force the call mode to routed when dialing out to H.460 clients.
DMA-7611	In some cases, after a DMA cluster left a supercluster, only two dashboard panes would appear.
DMA-7666	H.323 Routed call mode: External endpoints in same NAT failed to make call.
DMA-7720	When call history records were purged, some of the data wasn't removed.
DMA-7722	When a VCS is neighbored to DMA, the VCS sends probe LRQs to test DMA's availability. DMA failed to handle call history data for these probe LRQs properly, resulting in slow queries.
DMA-7748	Customers upgrading from v2.3 to v4.0 might have lost data as a result of the upgrade operation due to the system running out of memory during the upgrade process.

Issues Resolved in Version 4.0.2

The following table lists the issues resolved in the version 4.0.2 release.

Issue ID	Description
DMA-5961	When a SIP VVX1500 endpoint called an H.323 VVX1500 endpoint, and the endpoints were using the H.263 video codec, the H.323 endpoint didn't receive video.
DMA-6532	When an H.323 HDX endpoint called a SIP VVX endpoint, and the endpoints were using the H.264 video codec, the H.323 endpoint didn't receive video.
DMA-6553	In a Microsoft Lync environment, H.323 endpoints using the DMA system as a gateway were unable to connect to Lync clients. Note: See DMA-7303 above. Also, see DMA-7176 in the "Known Issues" list on page 25 for a related problem and its workaround.
DMA-6629	When an HDX endpoint using H.323 called a SIP HDX endpoint via the DMA gateway, and the endpoints were using 1080p, the H.323 endpoint didn't receive video.
DMA-6862	When restoring from a backup, one of the datastore processes sometimes became stuck.
DMA-6964	Bad performance of H.323 registration.
DMA-6968	Some configuration lost during upgrade to version 4.0.1.
DMA-6978	DMA outbound registration From: field didn't comply with mandatory parameters according to RFC3261.
DMA-6993	Dashboard: On "Call Server Active Calls" pane, the TOTAL numbers was greater than the sum of all the clusters.
DMA-7017	Unable to register on Exchange with error "Exchange Authentication failed" if NTLM v2 is forced.
DMA-7019	Call from H.323 EP which registered on CMA to SIP EP registered on DMA failed.
DMA-7021	Performance issues when a system was swarmed by registration requests on start-up.
DMA-7041	DMA did not maintain configuration and EP provisioning data after upgrade.
DMA-7088	When importing CMA site topology from CMA, DMA should adjust the values to reconcile the difference in bandwidth calculations.
DMA-7115	DMA v4.0.1 GA, server 2 got stuck when becoming the primary server.
DMA-7119	DMA cluster lost unexpectedly its call licenses (600 > 10).
DMA-7167	In some rare instances, data corruption may occur during upgrade.
DMA-7184	Leaking RAS transactions caused the GK to stop accepting registrations.
DMA-7187	When a certificate was loaded with a DirName SAN, the GUI could no longer access the certificates.
DMA-7188	NonRepudiation bit in CSR caused some CAs to not sign cert.

Issues Resolved in Version 4.0.1

The following table lists the issues resolved in the version 4.0.1 release.

Issue ID	Description
DMA-6272	When the DMA system attempted to register with an external SIP device or server, it didn't present its credentials if challenged.
DMA-6408	When a territory's backup cluster was serving as gatekeeper and the primary cluster restarted, the backup cluster sent URQs telling registered devices to re-register with the primary cluster before the primary cluster was ready to accept registrations.

Issue ID	Description
DMA-6412	When a territory's primary cluster was gracefully shut down, the backup cluster erroneously rejected lightweight registration requests (LWRRQs) from devices registered with the primary cluster. The backup cluster allowed devices to register only after they sent a full registration request.
DMA-6525	When a territory's primary cluster came back into service, it sent disengage requests (DRQs) to endpoints connected to an RMX conference room despite being in direct, not routed, mode.
DMA-6611	When embedded DNS was enabled or its domain field modified, the DNS service didn't start or restart until the system was rebooted.
DMA-6645	When it sent H.323 Annex O dial strings to a Tandberg VCS gatekeeper, the DMA system included only the user part of the URL in the request. The Tandberg VCS expects the whole URL, and the call failed.
DMA-6662	Alerts and daily statistics were not updating because the console service was blocked from starting due to socket bind issues.
DMA-6668	Calls from unregistered endpoints to endpoints registered to a neighbored gatekeeper failed the "Resolve to external gatekeeper" dial rule.
DMA-6699	When a territory's primary cluster received an LWRRQ from an HDX endpoint, it erroneously rejected it (rejectReason: fullRegistrationRequired). The endpoint then sent an RRQ to the backup cluster.
DMA-6716	The DMA system improperly handled multiple devices registering with the same SIP user name, instead of letting the last endpoint to register with a particular name prevail.
DMA-6726	When a territory's primary cluster rebooted, it didn't send URQs to endpoints in a call.
DMA-6737	Calls from a CTS system to an RMX MCU through the DMA system failed after a few seconds.
DMA-6751	The DMA system improperly handled some special characters in Active Directory group names, causing a cache load failure when a group name contained special characters.
DMA-6761	When a territory's primary cluster came back into service, the backup cluster sent URQs to endpoints and MCUs in a call.

What's New in the Version 4.0 Release

The Polycom DMA system version 4.0 includes the following new features. For more information on these new features, see the *Polycom DMA System Operations Guide* and the online help.

- Removal of legacy signaling mode

  The **Legacy signaling mode** setting (which turned off Call Server functionality) that was retained in version 3.0 to support customers upgrading from earlier versions has been removed. In this version of the Polycom DMA system, the Call Server is always enabled. It's no longer possible to register the system with another gatekeeper as a gateway/MCU. If you wish to use the system with another gatekeeper, you can neighbor to it rather than register with it.

  

  Upgrading a system without Call Server functionality to this version is a significant change that must be fully understood and planned for. It requires changes to your existing gatekeeper(s) and dial plan. Don't upgrade until you're prepared to use the Polycom DMA system as an H.323 gatekeeper and/or SIP registrar/proxy. See "Existing System Upgrade" on page 15.

- Registration with SIP peers

  This version of the Polycom DMA system supports registration with SIP devices/servers (such as the Acme SBC) that use registrations to dynamically configure routing rules and route specific calls to the registering SIP device. In a superclustered Polycom DMA system, registrations are assigned to DMA territories, so they can fail over to the backup cluster assigned to a territory when necessary.

- Gatekeeper support for IPv6

  This release extends the Call Server's H.323 gatekeeper functionality to networks using the IPv6 protocol.

- Registration control

  Registration control adds the ability to specify and enforce a policy governing endpoint registration. The policy is created by writing a Javascript that defines the criteria governing endpoint registration. For instance, it might specify that after a certain date, only already-registered endpoints may re-register, or that only a specified list of endpoints may register.

- New **Dashboard** panes

  The following new panes have been added to the **Dashboard**:

  - Cluster Info
  - Exchange Server Integration
  - CMA Integration
  - Active Directory Integration
  - Conference Manager History – Max Participants

  The legacy dashboard has been removed.

- History of system alerts

  The new **Alert History** page lets you view and search the history of all alerts that have occurred in the system.

- Maximum security mode

  This release provides a maximum security mode for UC APL environments, where the most stringent security protocols must be adhered to.

  Enabling the **Maximum security** setting is ***irreversible*** and has significant consequences. See "The Consequences of Enabling Maximum Security Mode" on page 13 for a complete list of the special security features enabled by this setting and the features that aren't supported in this mode.

  It's important to note that the Polycom DMA system version 4.0 release is not a maximum-security-only release. During initial setup, it can be configured for a lower security level (the **High security** or out-of-the-box default **Custom security** settings). You can switch the system to **Maximum security** at any time after initial installation.

- Support for new RMX conference settings

  This release adds two new conference template settings for features added in RMX v7.6:

  - **H.264 high profile —** Enables conferences in video switching mode (VSW) on RMX v7.6 MCUs with MPMx cards to use Polycom's bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode). All endpoints in such a

conference must support High Profile. Endpoints not connecting at the conference's exact line rate and resolution are connected in audio-only mode.

- **TIP compatibility** — Enables RMX v7.6 MCUs with MPMx cards to natively inter-operate with Cisco TelePresence® Systems (CTS), using Cisco's proprietary Telepresence Interoperability Protocol (TIP). Conferences can include both endpoints that don't support TIP and CTS endpoints.

- SIP interoperability enhancements

  This release incorporates a number of enhancements in its SIP signaling functionality that improve interoperability with third-party products. These enhancements include support for:
  - Cisco TIP
  - Microsoft OCS CAC-14
  - Avaya
  - Broadsoft
  - Siemens

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 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 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 IP address.
- SIP signaling 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 CMA system is not supported.
- Superclustering 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 **Tools** menu, **Top** is removed.
- In the **Add User** and **Edit User** dialog boxes, conference and chairperson passwords are obscured.
- After **Maximum security** is enabled, users must change their passwords.
- If the system is integrated with Microsoft 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).
- 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).
- 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 enterprise directory integration, the network between the DMA 7000 and the enterprise 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.
- 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).
- Minimum display resolution: 1280x1024 (1680x1050 recommended).

Installation and Upgrade Notes

New System Installation

Installation of new Polycom DMA 7000 systems is managed through Polycom Project Management. For more information, please contact your Polycom representative.

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

Existing System Upgrade

Polycom DMA systems running versions 2.3 or 3.0 (with or without service packs) can be upgraded to version 4.0.3 P3. This upgrade requires a new license key after the upgrade. Systems running version 4.0.x (with or without patches) can be upgraded without needing a new license key.

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

Customers upgrading a version 2.3 system, or a version 3.0 system that has Call Server disabled (the **Legacy signaling mode** option), must be prepared for the significant signaling changes introduced by the Call Server function (see "Call Server" on page 2 and "What's New in the Version 4.0 Release" on page 11).

When such a system is upgraded to version 4.0, the upgrade process adds any gatekeeper to which it was previously registered to the list of neighbor gatekeepers.

The neighbor gatekeeper(s) must then be reconfigured to treat the Polycom DMA system as a trusted neighbor and route calls to it. For a Polycom CMA system, this requires the following steps:

1. Log into the CMA system.
2. In **Network Device > DMAs**, delete the DMA entry.
3. In **Admin > Dial Plan and Sites > Services**, remove the service prefix (the dial prefix in the DMA system) with which the DMA system registered with this gatekeeper.
4. In **Admin > Gatekeeper Settings > Neighboring Gatekeepers**, add the DMA system as a neighbor.
5. In **Admin > Dial Plan and Sites > Dial Rules**, add a dial rule with the following settings:

   Pattern Type: Prefix

   IP Address Pattern Data: The dial prefix of the DMA system

   Action: Route to a trusted neighbor

   Trusted Neighbor: The entry you created for the DMA system (step 4)

See the *Polycom CMA System Operations Guide* for more information about neighboring gatekeepers.

For other gatekeepers, the specific steps will differ, but the same tasks must be completed. See the documentation for your gatekeeper.

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 2010 integrations. For more 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.

Note: 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).

IRQ/IRR Handling

The Polycom DMA gatekeeper sends an Information Request (IRQ) message to an endpoint when it first registers with the gatekeeper. If the endpoint responds with an Information Request Response (IRR) to the initial request, the DMA gatekeeper marks that the endpoint has the ability to process IRQs.

For endpoints that DMA has determined support IRQs, DMA sends an IRQ message at the interval specified in the IRQ sending interval (seconds) on the **Admin->Call Server->Call Server Settings** page.

If the endpoint responds to that IRQ with an IRR indicating invalid call or with no call information, the new setting on the **Call Server Settings** page (added in 4.0.3 P1; see page 3) determines whether the DMA gatekeeper terminates the call.

If you have endpoints that you know or suspect don't properly handle IRQ/IRR, leave **Terminate calls based on failed responses to IRQs** turned off.

Device Version Compatibility

The following list is not a complete inventory of compatible equipment. It simply indicates the products that have been tested for compatibility with the Polycom DMA system version 4.0 release. For more information about partner product interoperability, refer to the partner deployment guides.

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.

Device	Version	Notes
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	L6.0, L6.1	
Cisco (Tandberg) 6000 B Series	EB10.3	
Cisco (Tandberg) 6000 E Series	E5.3	
Cisco (Tandberg) C20	4.1.1, 4.1.2	
Cisco (Tandberg) C90	4.1.1, 4.1.2	
Cisco (Tandberg) E20	4.0.0	
Cisco (Tandberg) EX90	4.1.1, 4.1.2	
Cisco (Tandberg) GK	N6.1	
Cisco (Tandberg) MCU 4210	4.0, 4.1, 4.2	
Cisco (Tandberg) MCU 4505	4.0, 4.1, 4.2	
Cisco (Tandberg) Codian MSE Supervisor 8050	2.2	
Cisco (Tandberg) Codian MSE 8510	4.1	
Cisco (Tandberg) Codian MSE 8420	4.0	
Cisco (Tandberg) MXP	F9.0, F9.1	
Cisco 3745 GK	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.
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.

Device	Version	Notes
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 Room	4.7.17(1)	
Lifesize Team 220	4.8.0(59)	
Microsoft Lync		Please consult the Polycom UC Deployment Guide for Microsoft Environments for a list of supported versions and interoperability scenarios.
Polycom CMA	5.x, 6.x	
Polycom CMAD	5.x	
Polycom DST B5	2.0	
Polycom DST K60	2.0.1	
Polycom FX	6.0.5	
Polycom HDX	2.x.y, 3.x.y	
Polycom iPower 9000	6.2.0	
Polycom ITP (RPX, APX, OTX)	3.0.3	
Polycom m100	1.0	
Polycom MGC 50+	9.0.4.3	
Polycom PathNavigator	7.00.12	
Polycom PVX	8.0.4, 8.0.16	
Polycom QDX4000	4.0.1.1	
Polycom RMX1000	2.1	
Polycom RMX1500, 2000, 4000	6.x, 7.x	
Polycom SE200	3.00.07	
Polycom SoundPoint 601/650 SIP	3.3.1	
Polycom V500	9.0.6.1	
Polycom VS	7.5.4	
Polycom VSX	9.0.6.1	
Polycom VVX1500	4.0.1	Versions prior to 4.0.1 don't handle IRQ/IRR correctly.
Radvision ECS GK	5.6.2.10, 7.1.2.12	
Radvision Scopia XT1000	2.0.115	
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.

Device	Version	Notes
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	2.30, 2.72	
Sony PCS-TL50	2.42	
Sony PCS-XG80	2.30	

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	Version	License	Link
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	5.6	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
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

Software	Version	License	Link
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
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
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	1.6.0.20	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
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
libesmtp	1.0.4	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
libnet	1.1.4		

Software	Version	License	Link
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
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
OpenDS	2.2.0	CDDL	http://www.opensource.org/licenses/cddl1.php
openSSH	Part of Centos distribution	OpenSSH	http://www.openssh.org
openSSL	Part of Centos distribution	OpenSSL	http://www.openssl.org/source/license.html
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
Snmp4j	1.10.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
sudo	1.7.2p1	ISCL	https://www.isc.org/software/license
Xerces2	See JBoss.	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
OpenFire		Apache License, Version 2	http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html
Rhino		Mozilla Public License, v1.1	http://www.mozilla.org/MPL/MPL-1.1.html https://developer.mozilla.org/en/Rhino_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/ http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html
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			
CS CodeViewer	v1.0	BSD-like	
Crimson	v1.1.1	Apache 1.1	
Xalan J2		Apache 2.0	
NSIS	1.0j	(see license file)	
IAIK PKCS Wrapper		BSD-like	

Software	Version	License	Link
Document Object Model (DOM)	v. Level 3	W3C SOFTWARE NOTICE AND LICENSE	
Xalan, Xerces		Apache 1.1	
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	
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])	
Byte Code Engineering Library (BCEL)	v. 5	Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
CUP Parser Generator for Java	v. 0.10k	(general permissive license)	
JLex: A Lexical Analyzer Generator for Java	v. 1.2.5	(general permissive license)	
SAX	v. 2.0.1	Public Domain	
Cryptix		Cryptix General License	
W3C XML Schema Test Collection		W3C DOCUMENT NOTICE AND LICENSE	
Stax API		BEA License (unique terms)	
X Window System		(general permissive license)	
dom4j v. 1.6		BSD-like	
Retroweaver		(general permissive license)	
Stripper		BSD-like	
libpng official PNG reference library		(general permissive license)	

Software	Version	License	Link
Libungif – An uncompressed GIF library		(general permissive license)	
Ant		Apache 2.0	
XML Resolver Library		Apache 2.0	
ICU4J		ICU License	
NekoHTML		Apache-like (1.1)	
Jing		(general permissive)	
RelaxNGCC		(general permissive)	
RELAX NG Object Model/Parser		MIT License	
XFree86-VidMode Extension		Version 1.1 of Project Licence (BSD-like)	
RelaxNGCC		version 2003-May-08 of the Info-ZIP copyright and license	ftp://ftp.info-zip.org/pub/infozip/license.html
XML Security		Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
Zlib		(general permissive)	
Mozilla Rhino		Netscape Public License Version 1.1	
Apache Derby		Apache 2.0	
7-Zip		(see file) Some files are LGPLv2.1; some have the unRAR restriction; some are licensed under AES code license	
UPX		GPL	
LZMA Software Development Kit		Common Public License (CPL)	

Resolved Issues

The following table lists the issues resolved in the Polycom DMA 7000 system version 4.0 base release. See the "What's New" sections starting on page 3 for issues resolved in the subsequent maintenance releases.

Issue ID	Found in Version	Description
DMA-1678	2.0	If one server of a two-server DMA system is down, and the other server terminates integration with a CMA system, the system re-integrates with the CMA system when the second server is powered back on.
DMA- 2353	2.3	In some situations, SIP calls from an HDX endpoint to an existing RMX conference room joined with only video - no audio.
DMA- 2366	2.3	In some situations, SIP calls from an RMX to an HDX registered with a Tandberg VCS gatekeeper failed.
DMA-2700	2.3	If the DMA system applied a postliminary transformation to a dial string before sending the call to a neighbored CMA GK, the call sometimes failed.
DMA- 2743	2.3	SIP calls failed if they spanned two DMA clusters that both had transport protocol set to Auto.
DMA-3142	2.3	If the system's network configuration was changed to IPv6 addressing only, but no IPv6 address was specified, the system became unreachable. The system now presents an error message and prevents this misconfiguration.
DMA-3454	2.2	Failure to specify NTP servers sometimes led to a time disparity on the two servers of a two-server cluster. Now, if no NTP server is specified, Server 2 syncs its clock to Server 1. We still strongly recommend that you specify at least one and preferably three NTP servers.

Known Issues

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

Issue ID	Found in Version	Description	Workaround
DMA-1527	2.0	When the DMA system is using a Radvision ECS GK set for routed mode, endpoints are displayed twice on the RMX's EMA.	Configure the Radvision ECS GK to use direct mode routing.
DMA-1691	2.0	Calls from Tandberg 6000 E and 6000 B endpoints are unable to join a DMA meeting.	
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. Use of this feature is not recommended, however, because support for it varies significantly among different kinds of endpoints.

Issue ID	Found in Version	Description	Workaround
DMA- 2014	2.3	Polycom HDX and PVX endpoints don't support failover of SIP registrations.	
DMA-2109	2.3	Polycom V500 endpoints don't support failover of SIP registrations.	
DMA- 2362	2.3	In some situations, SIP calls from an RMX to an HDX join with only video - no audio.	
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- 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: Disable cascading for the conference while the GK is unavailable. Register the RMX to a working GK. Busy out the RMX while its GK is unavailable.
DMA- 2797	2.3	Some Sony endpoints that register with the DMA system become unregistered after five minutes.	
DMA- 3390	2.3	If a DMA cluster is the primary or backup for a territory, it can 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- 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- 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- 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- 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- 5069	3.0	In a superclustered environment, slight time drifts between clusters may produce CDR records out of order or duplicated. 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. No loss of functionality or data occurs as a result of this issue.
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- 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-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-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-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-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-6469 DMA-6472	4.0	In a SIP to H.323 call through the DMA system's gateway, the H.323 endpoint transmits video in H.263 CIF at bit rates up to 6144 kbps.	

Issue ID	Found in Version	Description	Workaround
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.	
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-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-6524, 8102, 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-6598	4.0	If a two-server cluster is configured without using the USB stick (the alternate procedure in the *Getting Started Guide*), but Server 2 is running while Server 1 is being configured, the two servers can end up not synchronized and not clustered. This leaves the system in an unusable state.	To avoid this problem, follow the procedure in the *Getting Started Guide*, which requires that Server 2 not be turned on until Server 1 has been configured, finishes rebooting, and displays **DMA Ready** on the LCD. To recover from this problem: Turn off Server 2. Reboot Server 1, and wait for it to finish rebooting and display **DMA Ready** on the LCD. Turn on Server 2. It detects and gets its configuration settings from Server 1 and joins the cluster. When done, both servers' LCDs display **DMA Clustered**.
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. Other gatekeepers, such as CMA and VCS, treat dial strings of the form "<user>@<domain>" as url-IDs. The DMA system's different treatment of these dial strings means that calls to non-neighbored external gatekeepers are likely to fail. 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: DIAL_STRING=DIAL_STRING.replace(/^([^:@]*)@([^@]*)/,"h323:$1@$2");
DMA-7073	4.0.1	SIP endpoints remain listed as inactive (although actually active) after a territory failover.	

Issue ID	Found in Version	Description	Workaround
DMA-7131	4.0.1	A VBP allows endpoints on external networks to register through it to a LAN-side gatekeeper (DMA). It does this by proxying H.323 events from the public network to an internal network. On the LAN side, 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). As a result, DMA displays all VBP calls as having the same endpoint information as the device that originally sent the successful registration to the DMA (and was assigned the endpoint identifier in the RCF).	
DMA-7168	4.0.1	HDX or Lync SIP calls to encrypted VMRs via a VEQ are hooked when being transferred to the VMR.	Use an unencrypted VMR.
DMA-7176	4.0.2	Despite the fix for DMA-6553, some calls from HDX endpoints using the DMA system as a gateway to Lync clients fail (Ms-client-diagnostics: 52001; reason= "Client side general processing error.").	Have the Lync user call the HDX endpoint.
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-7297	4.0.2	After upgrading a DMA currently integrated with an AD server to v4.0.x, a user might not be able to log into the DMA GUI via an AD account.	Log in as a local user and update the AD integration by simply clicking the Update button on the Microsoft Active Directory Integration page.
DMA-7369	4.0.2	Calls fail for registered Real Presence Mobile endpoints using dial strings of the form "<IP Address>##<Alias>" to make H.323 calls to external networks, using a VBP-E as a Session Border Controller.	
DMA-7418	4.0.3	Deselecting the "Allow calls to/from rogue endpoints" option prevents calls to endpoints in the configured site topology that are not registered to the DMA, even when the endpoints are registered to a neighbored gatekeeper or SIP peer and the neighboring or peering dial rule is used to route the call.	
DMA-7436	4.0.3	When the primary cluster for a territory is changed, there is no warning dialog explaining that endpoints that were registered will become inactive until they re-register.	

Issue ID	Found in Version	Description	Workaround
DMA-7466	4.0.3	When the DMA receives a call from a SIP proxy and attempts to connect the call to one of its endpoints, if bandwidth management logic rejects the call after the dialed endpoint responds with a SIP 200 OK message (when the line goes off-hook), the DMA terminates the call to that endpoint but not to the calling leg. The calling leg sends 200 OK messages until timeout (less than 30 seconds), and only then does the call fail and resources get properly cleaned up.	
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-7548	4.0.3	If “Allow calls to/from rogue endpoints” is enabled, a call to a blocked endpoint in the Internet/VPN site succeeds.	
DMA-7567	4.0.3	Postliminary script for MCU isn’t saved.	Change the description or the name of the MCU and the postliminary will be saved.
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.	
DMA-7632	4.0, 4.0.1, 4.0.2	Territory delete doesn’t warn about or clean up users assigned to that territory.	
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-7695	4.0.2	High failure rate on SIP registrations from RMX MCUs.	
DMA-7712	4.0.2	If an RMX MCU was provisioned on the DMA system’s MCU page prior to the RMX registering to the DMA gatekeeper, the DMA gatekeeper could reject the registration.	Remove the RMX from the MCU page prior to registering it with the DMA gatekeeper.
DMA-7737	4.0.3	Call Forwarding On Busy doesn’t work when forwarding to endpoints not known to the DMA and registered to external proxies.	
DMA-7774, DMA-7784	4.0, 4.0.3	DMAs integrated to AD prior to upgrading might lose their connection to AD as a result of the upgrade to 4.0.3.	Log in as a local user and update the AD integration by simply clicking the Update button on the Microsoft Active Directory Integration page.

Issue ID	Found in Version	Description	Workaround
DMA-7812	4.0.3	For gateway calls between some endpoints, the video isn't displayed on one of the endpoints.	
DMA-7821	4.0.3	If you configure a prefix service for an MCU in the dial plan, you can't dial just the prefix to be routed to that MCU. You must dial something after the prefix value to be routed. This prevents the DMA from routing to the default entry queue on an RMX. Example: If an RMX has a prefix of 77 and an entry queue of 1000, you must dial 771000. Dialing 77 is not enough.	To reach the default entry queue on an RMX, dial it by its number or the RMX's IP address.
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." 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 don't.	Retry the integration until it succeeds. To avoid this form of cache loading failure, integrate to an AD server that has sufficient performance.

DMA-7831	4.0.3	When configuring an external gatekeeper with a prefix, a postliminary script is required to remove the prefix from the dial string that is forwarded to the external gatekeeper.
		A sample postliminary script is in the workaround field.
			if (DIAL_STRING.indexOf("sip:") == 0)
			{ DIAL_STRING = "sip:" + DIAL_STRING.substring(4 + <The length of the prefix string>, DIAL_STRING.indexOf('@')) + DIAL_STRING.substring(DIAL_STRING.indexOf('@')); }
			else
			{ DIAL_STRING = DIAL_STRING.substring(<The length of the prefix string>); }

DMA-7834	4.0, 4.0.3	In rare instances, an upgrade or rollback can result in not being able to log into the GUI as any user.	Reboot the DMA.
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.

Issue ID	Found in Version	Description	Workaround
DMA-8237	4.0.3	The number of calls displayed in the **Call History** page doesn't match the number included in the CDR export.	Make sure the search criteria specify calls completed during the same time span. On the **Call History** page: ▪ **End after** should match **Start date** in the **Export Time Frame** dialog. ▪ **End before** should match **End date** in the **Export Time Frame** dialog. ▪ **Start after** should be a very old date. ▪ **Start before** should be now or in the future.
DMA-8283	4.0.3	If a call's bit rate is reduced by endpoint negotiation, the DMA system doesn't show the correct bit rate.	
DMA-8450	4.0.1	Backup files larger than 2 GB can't be uploaded to the system.	
DMA-9115	4.0.3 P1	The DMA system creates an active call entry for an OCS chat INVITE.	
DMA-9118	4.0.3 P2	Call licenses are consumed by calls that never actually started (only ARQ/LRQ received) or failed to be cleaned up.	
DMA-9140	4.0.3	When SIP calls were made from CUCM to a DMA VMR, the conference created on the RMX had a random VMR number, not the VMR number dialed.	

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 4.0)

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 clicking "I AGREE" 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. Except as required under a Third Party License, 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 laws applicable, notwithstanding this limitation. 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.

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 Activities. 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 Activities"). POLYCOM AND ITS SUPPLIERS EXPRESSLY DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

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.

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

***

Portions of this SOFTWARE PRODUCT are © 2010 RADVISION Ltd. All rights reserved.

This SOFTWARE PRODUCT includes Berkeley DB Java Edition software. Copyright (c) 2002, 2008 Oracle. All rights reserved. Oracle is a third party beneficiary of this Agreement.
This SOFTWARE PRODUCT includes software having copyrights owned by, or licensed from, MySQL AB and Sun Microsystems.
* * *

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