Release Notes

Polycom® Distributed Media Application™ (DMA®) 7000 System, Version 5.0.2.1 Release

Polycom® announces the release of its Polycom® Distributed Media Application™ (DMA®) 7000 System, version 5.0.2.1. This document provides the latest information about this release.

Topics

Copyright Information

3725-76300-001T4 (04/2013)

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

Trademark Information

Introducing the Polycom DMA® 7000 System

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

Use of this software constitutes acceptance of the terms and conditions of the Polycom DMA 7000 system end-user license agreement on page 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 and 1200 concurrent conference (virtual meeting room, or VMR) calls.
- MCUs can be added on the fly without impacting end users and without requiring re-provisioning.

Call Server

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

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

Clustering and Superclustering

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

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

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

Other Key Features

The Polycom DMA 7000 system also:

- Integrates with Microsoft Active Directory, automating the task of provisioning users for video conferencing. Combined with its advanced resource management, this makes ad hoc video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.
- Integrates with Microsoft Exchange Server, enabling users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.
- Integrates with a Polycom RealPresence Resource Manager or CMA system to obtain site topology and user-to-device association data.

System Capabilities and Constraints

The following capabilities and constraints apply to the entire supercluster:

- Number of sites: 500
- Number of subnets: 5000
- Number of clusters in a supercluster: 5 (not counting an integrated Polycom RealPresence Resource Manager or CMA system)
- Number of MCUs enabled for conference rooms: 64
- Number of territories enabled for conference rooms (Conference Manager enabled): 3
- Number of concurrent VMR calls: 1200 per cluster (Conference Manager), up to 3600 total
- Number of concurrent SIP<->H.323 gateway calls: 500
- Size of Active Directory supported: 1,000,000 users and 1,000,000 groups (up to 10,000 groups may be imported)

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

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

What's New in the Version 5.0.2.1 Release

The Polycom DMA system version 5.0.2.1 is a maintenance release that fixes a number of issues found since the version 5.0.2 release. It replaces the version 5.0, 5.0.1, and 5.0.2 releases.

Issues Resolved in Version 5.0.2.1

The following table lists the issues resolved in the version 5.0.2.1 release.

Issue ID	Found in Version	Description
DMA-10979	5.0.2	The database purge utility, which removes the oldest history data to prevent the system from running out of disk space, was unable to keep up with the data arrival rate under heavy load.
DMA-10636, 9312	5.0	If either (a) the active server in a two-server cluster failed over to the backup server or (b) the primary cluster for a territory failed over to the backup cluster, a conference for which the failed server or cluster was responsible could continue without the backup server or cluster taking over signaling for it. If a new (or dropped) participant dialed into the same conference room (VMR), the backup server or cluster started a new conference. This resulted in two active conferences for the same VMR. To prevent such split conferences, when a server or cluster fails, the backup server or cluster contacts the MCU(s) to terminate the conferences for which the failed server or cluster was responsible (this may take up to two minutes). **Note:** Depending on the endpoint, when the conference is terminated, the endpoint's video may freeze instead of the call hanging up. The user can simply hang up and dial back in. When the participants in a conference dial back in, the backup server or cluster creates a new conference. **Note:** Some calls killed in this way may continue to appear on the Active Calls page for up to 30 minutes, depending on the number of such calls.
DMA-10561	5.2	The system leaked memory when an API client used certain conference commands.
DMA-10520	5.0.1 HF1	When DMA is neighbored to Avaya Communication Manager, H.323 calls from an RMX registered to the DMA to an Avaya Meeting Exchange failed to connect.
DMA-10468	5..2 HF2	For all point-to-point and some VMR calls, the system leaked memory in the call audit cache.
DMA-10360	5.0.2	The system rejected attempts to connect to the API via mutual TLS (mTLS).
DMA-10329	5.0.2	By design, before a search is conducted, the Call History page doesn't list any calls. But at the bottom of the page, it displayed a count of calls found. This was a raw count that summed the number of calls going through each cluster without consolidating the calls traversing more than one cluster, leading to confusion when the count changed after clicking the Search button. The raw count has been removed; now, a count of calls found appears only after a search is conducted.
DMA-10292	5.0.2	When the hub MCU of a cascaded conference became unavailable, the cascade links from spoke MCUs remained active. H.323 endpoints that were on the hub MCU couldn't dial back into the conference and hub failover didn't happen.
DMA-10198	5.0.2	When an ISDN endpoint called a VMR hosted on the same MCU whose ISDN gateway the call was using, the DMA system detected this as a loop, and the call failed.
DMA-10195	5.1	Searching registration history caused high CPU usage, triggering an alert.
DMA-10099	5.0.1	A DMA system in WAN-side gatekeeper mode occasionally blacklisted LAN-side H.323 endpoints registered via a VBP session border controller.

Issue ID	Found in Version	Description
DMA-10061	5.0.1	If the DMA system received URQs with no endpointIdentifier from a VBP session border controller, it failed to respond, leading the VBP to treat the DMA system as unavailable. This sometimes made it impossible for RealPresence Mobile devices behind the VBP to register with the DMA gatekeeper.

Issues Resolved in Version 5.0.2

The following table lists the issues resolved in the version 5.0.2 release. Except as indicated, these issues are also resolved in version 5.1.

Issue ID	Found in Version	Description
DMA-9895	5.0.1	A DMA system was configured to register with an external Broadsoft SIP peer. Outbound authentication was enabled. The Broadsoft server accepted the registration, specifying a 600-second registration expiration timer. The DMA system ignored that and re-registered much more frequently (1 to 2 per second). **Note:** This fix is not included in version 5.1.
DMA-9855	5.1	Certain H.323 endpoints attempting to reach a VMR via a VBP were rejected as not registered. They believed they're registered and keep trying (sending ARQ), and the DMA kept rejecting them (sending ARJ). This prevented the calls from completing, grew the database, and created lots of network traffic. **Note:** This fix is not included in version 5.1.
DMA-9806	5.0.1	After a failover, when the primary DMA cluster for a territory regained control of that territory, an H.323 endpoint sending a registration request (RRQ) to that cluster received a confirmation (RRJ) that didn't specify the backup cluster as the alternate gatekeeper.
DMA-9792	5.0	Registration issues with incorrectly named ITP endpoints caused multiple duplicate alerts.
DMA-9781	5.0.1	An HDX SIP endpoint with call speed set to AUTO called a PSTN device via the DMA system. The call was forwarded to a CUCM server and out the gateway to the PSTN network. The DMA system and HDX endpoint were both configured to accept a minimum call speed of 64k. The call appeared to set up properly, but there was no audio. **Note:** This fix is not included in version 5.1.
DMA-9778	5.0.1, 5.1	HDX endpoints were unable to register with the DMA gatekeeper because the DMA system was unable to look up the owner of the endpoint in the data returned from resource manager integration.
DMA-9734	5.0.1	The Dashboard on a DMA cluster incorrectly indicated that resource manager integration was disabled because it failed to check with all clusters in the supercluster.
DMA-9709	5.0	The DMA system didn't monitor the status of the OpenDJ (ldap) service and restart it when it stopped.
DMA-9672	5.0.1	A memory leak during the processing of SIP VEQ calls caused a DMA cluster to fail. **Note:** This fix is not included in version 5.1.
DMA-9650		Calls to the DMA system via a Genband A2 SIP call server were dropped. The DMA system was incorrectly terminating a call when it received a SIP INFO message with empty content from the Genband A2 SIP call server.
DMA-9647	5.0.1, 5.1	The web UI throws error 'The file could not be downloaded.' when attempting to download CDR data. This happens when the CDR web-page is being accessed from a machine that currently has GMT+ time (positive GMT offset). This issue now has been fixed.

Issue ID	Found in Version	Description
DMA-9641	5.0.1	In a superclustered configuration where an external gatekeeper is neighbored to cluster 1, each time an endpoint registered to the neighbor GK calls into a VMR hosted by cluster 2, a call license is leaked on cluster 1 and a phantom call is added to the Active Calls pane on the Dashboard.
DMA-9613	5.0	Various interoperability issues were discovered involving gateway calls from or to Sony PCS-XG80, Cisco EX90, and Cisco (Tandberg) MXP 6000 endpoints. To avoid problems with these endpoints, on the Call Server Settings page turn off Terminate calls based on failed responses to IRQs. **Note:** This fix is not included in version 5.1.
DMA-9593	4.0.3 P4, 5.1	The Active Calls pane on the Dashboard sometimes showed phantom calls that didn't go away until the cluster was rebooted.
DMA-9547	5.0.1	Conference and chairperson passcodes that came from Active Directory integration couldn't be overridden in the Edit User or Add/Edit Conference Room dialogs.
DMA-9541	5.0, 5.1	Calls to a VMR managed by one territory and landing on an RMX MCU managed by another territory failed.
DMA-9537	5.0.1	The emergency purge script that runs when the disk is too full failed to delete old call signaling event audit records. **Note:** This fix is not included in version 5.1.
DMA-9509	5.0	After a software upgrade, all the backup files from the previous version remained on disk, consuming significant disk space. Now, only the backup performed as part of the upgrade process (needed in case of rollback) is retained.
DMA-9431	4.0.3	When a cluster served as the backup cluster for the territory responsible for resource management server integration, it took over the territory after a single failed ping of the primary cluster instead of waiting for the territory failover delay interval.
DMA-9430	4.0.3	Each time the Join Resource Management Server action was performed, the system started three threads. These threads were not cleaned up when the Leave Resource Management Server action was performed, causing a thread leak.
DMA-9428	4.0.3 P4	The table that stores call signaling event audit records could grow without bounds, causing backup sets to be huge and potentially causing the system to run out of disk space or upgrades to fail. The system now stops auditing lower priority call events (for SIP INFO and NOTIFY of SUBSCRIBES; for H.323, H.245 and IRQ and RAS INFO messages) for a call after a certain threshold is reached.
DMA-9391	5.0.1	The system was configured for shared number dialing, a dialing prefix was specified in Conference Settings, and VMR numbers coincidentally started with the same digits as the dialing prefix. The system improperly removed the prefix value when resolving the VMR number, causing calls to fail.
DMA-9351	5.0	API: 500 Internal Server Error when querying conference templates.
DMA-9142	5.0	An API client attempted to start a conference, and the DMA system returned a 503 error indicating insufficient MCU resources when that wasn't the case. (Resolved as not reproducible.)
DMA-9118	4.0.3 P2	Call licenses were consumed by calls that never actually started (only ARQ/LRQ received) or failed to be cleaned up.
DMA-8936	5.0	On point-to-point calls between Interactive Telepresence (ITP) systems, the ITP codecs (endpoints) sometimes connected at different bit rates. **Note:** This fix is not included in version 5.1.
DMA-7706	4.0.1	In certain error-handling scenarios, the system sometimes leaked memory, threads, or resources.
DMA-7695	4.0.2	High failure rate on SIP registrations from RMX MCUs.

Issues Resolved in Version 5.0.1

The following table lists the issues resolved in the version 5.0.1 release.

Issue ID	Found in Version	Description
DMA-9218	4.0.3 P3, 5.0	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.
DMA-9196	5.0	Upgrading to 5.0.0 from a previous version could cause the audit subsystem to fail.
DMA-9164	4.0.3 P2, 5.0	If an RMX MCU registered with the DMA Call Server as a SIP device (in order to make SIP dial-outs) and was also added to the DMA Conference Manager's pool of conferencing resources, the DMA system had two records of the MCU and didn't connect those records. ▪ On the MCUs page, the MCU always had a registration status of inactive. ▪ On the Endpoints page, the MCU appeared as an endpoint with a SIP URI and its actual registration status. If the MCU's registration was blocked, quarantined, deleted, or rejected, SIP dial-outs failed.
DMA-9100	4.0.3 P1	When a cluster was removed from the supercluster and its territory responsibilities reassigned, some endpoint registrations could get stuck in an active state.
DMA-9063	5.0	When recording a DMA VMR (virtual meeting room) conference, the pause command didn't work.
DMA-9062	4.0.3 P1	AD integration: Using directory attribute other than "telephoneNumber" failed to associate any conference rooms to users until reboot.
DMA- 9035	5.0	In some versions of Windows, when a Lync 2010 client was in a call with a Cisco C40 endpoint, the video sometimes froze.
DMA-8998	5.0	On a point-to-point call from a Lync 2010 client to an X-Lite software endpoint, the Lync 2010 user didn't receive video.
DMA-8959	5.0	When a call began as audio only, but later upgraded to video, the call history failed to record the change.
DMA-8856	5.0	On the Call Info tab of the Call Details dialog box, the final dial string value was sometimes incorrect or missing.
DMA-8825	5.0	When a call traversed two or more DMA clusters within one second, the call records from the clusters weren't always merged correctly, leading to inconsistent Call History information. **Note:** This problem is resolved for callers managed by one of the clusters in the supercluster, but not for rogue or neighbored calls (see DMA-9324 in the Known Issues list on page 25).
DMA-8237	4.0.3	Due to time zone issues and a CDR export problem, a CDR export sometimes included the wrong calls or was missing calls that should have been included. **Note:** The issues have been fixed, but in order for the same calls to appear in both the **Call History** page and the CDR export, but it's still important to be 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.

What's New in the Version 5.0 Release

The Polycom DMA system version 5.0 includes the following new features (portions of these were implemented in v4.0.3). For more information on these new features, see the *Polycom DMA 7000 System Operations Guide* and the online help.

- Application Programming Interface (API)

  This release includes the RealPresence Platform API, which provides programmatic access to the Polycom DMA system for the following:

  - Provisioning
  - Conference control and monitoring
  - Call control and dial-out
  - Billing and usage data retrieval
  - Resource availability queries

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

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

An API license isn't required in order for a Polycom RealPresence Resource Manager system to access the API. It's only needed for a client application you or a third party develop.

- SNMP support

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

  The system supports SNMPv3 communications with authentication and privacy.

- 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) and locally provisioned credentials.
  - Outbound authentication with external SIP peers using the SIP digest authentication mechanism and locally provisioned credentials.

  If inbound authentication is enabled for the system, it can be turned on or off for individual endpoints from the Endpoints page.

- Settings for stripping prefixes

  In this version of the Polycom DMA system, external devices that can be prefix services (SIP peers, gatekeepers, SBCs, and MCUs) can be configured to have the prefix stripped when a call that includes a prefix is routed to the device.

- 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 several 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.

- Other SIP enhancements

  Support has been added for the following:

  - DNS SRV failover (RFC 3263)
  - Refer (RFC 3515) (for blind transfer only)
  - External endpoint registration and keep-alive timer (RFC 5626) (TCP only, not UDP)
  - Loop/spiral detection and support for Max-Forwards and Max-Breadth headers (RFC 5393)

- Enhanced ITP support

  This release supports the new naming convention for the individual endpoints making up an Interactive Telepresence (ITP system) and provides bandwidth management for ITP calls.

- 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

  Internal 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 and to edit specific settings for 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.

Software Version History

Version	Release Date	Features
5.0.2.1	April 2013	Maintenance release to fix specific issues.
5.2.1	March 2013	Maintenance release to fix specific issues.
5.2.0	December 2012	Cascading for size, mixed AVC/SVC conferences, FW NAT keep-alive, improved subscription events reporting, new MCU support, enhanced API control of MCUs, removal of XMPP server.
5.0.2	December 2012	Maintenance release to fix specific issues.
5.1.0_P1	December 2012	Maintenance release to fix specific issues.
5.1.0	November 2012	SVC conferencing, RFC 4575 support, untrusted traffic identification and handling, network setting changes, upgrade process monitoring, and configuration-only backups.
5.0.1	September 2012	Maintenance release to fix specific issues.
4.0.3_P4	August 2012	Maintenance release to fix specific issues.
5.0.0	July 2012	RealPresence Platform API, SNMP support, device authentication enhancements, SIP enhancements, log forwarding, ITP support enhancements, and performance improvements.
4.0.3_P3	July 2012	Maintenance release to fix specific issues.
4.0.3_P2	July 2012	Not released for General Availability.
4.0.3_P1	May 2012	Maintenance release to fix specific issues, plus new call server option and subnet naming.
4.0.3	March 2012	Maintenance release to fix specific issues, plus authentication, SIP peer and endpoint enhancements, AD integration and database performance improvements, and new registration policy script variable.
4.0.2	February 2012	Maintenance release to fix specific issues.
4.0.1	December 2011	Maintenance release to fix specific issues.
4.0.0	October 2011	Registration control, GK IPv6 support, Dashboard enhancements, SIP interoperability enhancements, maximum security mode.
3.0.0_P1	September 2011	Maintenance release to fix specific issues.
3.0.0	July 2011	Call Server, superclustering, Juniper SRC integration, new Dashboard, new reporting and monitoring pages, new licensing.

The Consequences of Enabling Maximum Security Mode

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

- All unencrypted protocols and unsecured access methods are disabled.
- The boot order is changed and USB ports are disabled so that the server(s) can't be booted from the optical drive or a USB device.
- A BIOS password is set.
- The port 443 redirect is removed, and the system can only be accessed by the full URL (https://<IP>:8443/dma7000, where <IP> is one of the system's management IP addresses or a host name that resolves to one of those IP addresses).

- For all server-to-server connections, the system requires the remote party to present a valid X.509 certificate. Either the Common Name (CN) or Subject Alternate Name (SAN) field of that certificate must contain the address or host name specified for the server in the Polycom DMA system.

  Polycom 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.
- Superclustering is not supported.
- The Polycom DMA system can't be integrated with Microsoft Exchange Server and doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.
- Integration with a Polycom RealPresence Resource Manager or CMA system is not supported.
- On the **Banner** page, **Enable login banner** is selected and can't be disabled.
- On the **Login Sessions** page, the **Terminate Session** action is not available.
- On the **Troubleshooting Utilities** menu, **Top** is removed.
- In the **Add User** and **Edit User** dialog boxes, conference and chairperson passwords are obscured.
- After **Maximum security** is enabled, users must change their passwords.
- If the system is not integrated with Active Directory, each local user can have only one assigned role (Administrator, Provisioner, or Auditor).

  If some local users have multiple roles when you enable the **Maximum security** setting, they retain only the highest-ranking role (Administrator > Auditor > Provisioner).
- If the system is integrated with Active Directory, only one local user can have the Administrator role, and no local users can have the Provisioner or Auditor role.

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

  Each enterprise user can have only one assigned role (Administrator, Provisioner, or Auditor). If some enterprise users have multiple roles (or inherit multiple roles from their group memberships), they retain only the lowest-ranking role (Administrator > Auditor > Provisioner).
- Local user passwords have stricter limits and constraints (each is set to the noted default if below that level when you enable the **Maximum security** setting):
  - Minimum length is 15-30 characters (default is 15).
  - Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).
  - Maximum number of consecutive repeated characters is 1-4 (default is 2).
  - Number of previous passwords that a user may not re-use is 8-16 (default is 10).

- Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).
- Password may not contain the user name or its reverse.
- Maximum password age is 30-180 days (default is 60).
- Minimum password age is 1-30 days (default is 1).

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

  Session configuration limits:

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

  Local account configuration limits:

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

- Software build information is not displayed anywhere in the interface.
- You can't restore a backup made before the **Maximum security** setting was enabled.
- File uploads may fail when using the Mozilla Firefox browser unless the proper steps have been taken. See the *Polycom DMA 7000 System Deployment Guide for Maximum Security Environments*, the *Polycom DMA 7000 System Operations Guide*, or the online help.

System Requirements

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

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

Installation and Upgrade Notes

New System Installation

Installation of new Polycom DMA 7000 systems is managed through Polycom 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 3.0 or 4.0 (with or without service packs) can be upgraded to version 5.0.2.1. This upgrade requires a new license key after the upgrade. Systems running versions 5.0, 5.0.1, or 5.0.2 can be upgraded to version 5.0.2.1 without requiring a new license key.

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

Special Considerations for Upgrading from Version 3.0

Customers upgrading 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).

When such a system is upgraded, 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 integrations. For additional information, please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Interoperability

Integration with Polycom MCUs

To support the Polycom DMA system's **High security** setting, configure the Polycom RealPresence® Resource Manager and 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 a Polycom MCU conference profile. If you link templates to conference profiles, make sure the profiles exist and are defined the same on all the Polycom 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 *Administrator's Guide* for your MCU for more information on enabling encrypted connections and creating conference profiles.

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

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

If the conference template selected for a conference specifies mixed AVC and SVC mode, the DMA system doesn't limit the choice of MCU to those that support mixed mode. If the MCU selected doesn't support SVC at all, the DMA system starts the conference as an AVC-only conference. Otherwise, it starts a mixed mode conference. If the MCU doesn't support the mixed mode specified in the template, the conference simply doesn't start.

Polycom MCU Features Not Available in DMA System Templates

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

- **Customized Content Rate**

  In a conference profile on the MCU, this new option allows a custom content bit rate to be specified. To use this option via the DMA system, link the conference template to a conference profile that implements the custom setting.

  The existing Content Settings options (Graphics, Hi Res Graphics, and Live Video), which automatically determine the bit rate allocation for content, are available via the DMA system's standalone conference templates.

- **Mute participants except lecturer**

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

- **FW NAT keep alive**

  In a conference profile on the MCU, if this new Advanced option is selected, firewall/NAT traversal keep-alive messages are enabled and you can specify the message interval. To use this option via the DMA system, link the conference template to a conference profile that enables this option and the desired interval.

Products Tested with This Release

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

Go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html to see the Current Interoperability Matrix. You are encouraged to upgrade all your Polycom systems with the latest software before contacting Polycom support to ensure the issue has not already been addressed by software updates.

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.

Device	Version	Notes
Avaya Aura System Manager		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
Avaya One-X Communicator		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
BroadSoft BroadWorks Application Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
BroadSoft BroadWorks Media Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
BroadSoft BroadWorks Network Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
Cisco (Tandberg) 150 MXP	L6.0, 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, 5.0.1	
Cisco (Tandberg) C40	5.1	Some Cisco endpoints, including the C40, might experience problems establishing gateway calls (calls where the endpoints are using different protocols) with other 3rd-party endpoints, such as LifeSize Room 200 and Team 220 endpoints.
Cisco (Tandberg) C90	4.1.1, 4.1.2, 5.0.1	
Cisco (Tandberg) E20	4.0.0, 4.1.1	
Cisco (Tandberg) EX90	4.1.1, 4.1.2, 5.0.1	
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, F9.1.1	
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.

Device	Version	Notes
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.
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), 4.7.19(3)	
LifeSize Room 200	RM2_4.7.20	LifeSize Room 200 endpoints might experience problems establishing gateway calls (calls where the endpoints are using different protocols) with some Cisco endpoints, such as the C40.
LifeSize Team 220	4.8.0(59), 4.9.0(73)	LifeSize Team 220 endpoints might experience problems establishing gateway calls (calls where the endpoints are using different protocols) with some Cisco endpoints, such as the C40.
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	5.1, 5.2	
Polycom DST B5	2.0.1	
Polycom DST K60	2.0.1	
Polycom FX	6.0.5	
Polycom HDX	3.0.x	
Polycom iPower 9000	6.2.1208	
Polycom ITP (RPX, APX, OTX)	3.0.3, 3.0.4, 3.0.5	
Polycom m100	1.0	
Polycom MGC 50+	9.0.4.3	Can register with Call Server as free-standing MCU/gateway, but can't be added to Conference Manager's conferencing resource pool.

Device	Version	Notes
Polycom PathNavigator	7.0.14	
Polycom PVX	8.0.4, 8.0.16	
Polycom QDX4000	4.0.1.1, 4.0.2	
Polycom RealPresence Mobile	1.3	
Polycom RealPresence Resource Manager	7.0.0	
Polycom RMX1000	2.1	Can register with Call Server as free-standing MCU/gateway, but can't be added to Conference Manager's conferencing resource pool.
Polycom RMX1500, 2000, 4000	6.x, 7.x	
Polycom SE200	3.00.07	
Polycom SoundPoint 601/650 SIP	3.3.1, 4.0.1	
Polycom V500	9.0.6.1	
Polycom VS	7.5.4	
Polycom VSX	9.0.6.2	
Polycom VVX1500	4.0.1	Versions prior to 4.0.1 are not compatible due to a VVX defect. See DMA-6749 in the "Known Issues" list on page 25.
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.
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, 2.31	
X-Lite software SIP phone	5.0	Some compatibly issues have been found when making calls to a Polycom HDX in SIP mode and to a LifeSize Room200 in H.323 mode.

Open Source Software

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

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

Software Name	Version	License type	Source
Axis	1.4.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
bsf	2.3.0-rc1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
CentOs	5.8	GPLv2	https:/www.redhat.com/licenses/gpl.html
Cluster-glue	1.0.5	GPLv2	http://www.gnu.org/licenses/old-licenses/gpl-2.0.html
commons-beanutils	1.7	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-collections	3.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-configuration	1.5	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-digester	1.6	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-discovery	0.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-fileupload	1.2.1	Apache License, Version 2	http://commons.apache.org/fileupload/license.html
commons-httpclient	3.0.1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-io	1.4	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-jexl	1.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-jxpath	1.2	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-lang	2.3	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-logging	1.0.4	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
commons-pool	1.3	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
corosync	1.2.5	BSD	http://opensource.org/licenses/bsd-license.php
CXF	2.2.3	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
dom4j	1.5.2	BSD-style	http://www.dom4j.org/license.html
drools	4.0.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
generateDS	2.7a	MIT license	http://www.opensource.org/licenses/mit-license.php

Software Name	Version	License type	Source
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
jaxb2	0.6.0	BSD-style	http://confluence.highsource.org/display/J2B/License
JBOSS AS	4.2.1 GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-aop	1.5.5	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-cache	1.4.1.sp14	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-jaxws	2.0.0.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-jmx	4.2.1.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-remoting	2.2.2.sp1	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jboss-serialization	4.2.1.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
Jgroups	2.4.8.GA	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
jcifs	1.3.2	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
jna	3.0.9 b0	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
joesnmp	0.3.4	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
JSR 311	1.1.1	CDDL-1.0	http://www.opensource.org/licenses/cddl1.php
libesmtp	1.0.4	LGPLv2.1	http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html
libnet	1.1.4		
libxml2	1.2.3	MIT License	http://www.opensource.org/licenses/mit-license.html

Software Name	Version	License type	Source
Log4j	1.2.14	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
Neethi	3.0.1	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
NSS	Part of Centos distribution	Mozilla Public License v1.1	http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1
NSS Tools	Part of Centos distribution	Mozilla Public License v1.1	http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1
NTP	Part of Centos distribution	Open Software License v3.0	http://www.opensource.org/licenses/ntp-license.php
OpenDJ	2.5.0	CDDL-1.0	http://www.opensource.org/licenses/cddl1.php
OpenFire		Apache License, Version 2	http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html
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
Rhino		Mozilla Public License, v1.1	http://www.mozilla.org/MPL/MPL-1.1.html https://developer.mozilla.org/en/Rhino_License
sudo	1.7.2p1	ISCL	https://www.isc.org/software/license
Web App Solution, Inc. Flex 3 dashboard		Creative Commons Attribution-Noncommercial-Share Alike 3.0 Unported License, with a Creative Commons Plus License for commercial rights to the work.	http://creativecommons.org/licenses/by-nc-sa/3.0/ http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html
Xerces2	See JBoss.	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
xmlschema	2.0	Apache License, Version 2	http://www.apache.org/licenses/LICENSE-2.0
The Open Source packages below are included in the Polycom DMA 7000 system as a consequence of being embedded in the Java Platform, Standard Edition Embedded, version 6.0. License text available at http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT			
7-Zip		Some files are LGPLv2.1; some have the unRAR restriction; some are licensed under AES code license (see files)	
Ant		Apache 2.0	

Software Name	Version	License type	Source
Apache Derby		Apache 2.0	
Byte Code Engineering Library (BCEL)	v. 5	Apache 1.1	
Crimson	v1.1.1	Apache 1.1	
Cryptix		Cryptix General License	
CS CodeViewer	v1.0	BSD-like	
CUP Parser Generator for Java	v. 0.10k	(general permissive license)	
Document Object Model (DOM)	v. Level 3	W3C SOFTWARE NOTICE AND LICENSE	
dom4j v. 1.6		BSD-like	
IAIK PKCS Wrapper		BSD-like	
ICU4J		ICU License	
Jing		(general permissive)	
JLex: A Lexical Analyzer Generator for Java	v. 1.2.5	(general permissive license)	
libpng official PNG reference library		(general permissive license)	
Libungif – An uncompressed GIF library		(general permissive license)	
LZMA Software Development Kit		Common Public License (CPL)	
Mesa 3-D graphics library	v. 5	The core Mesa library is licensed according to the terms of the XFree86 copyright (an MIT-style license). The Mesa source code is licensed under SGI FREE SOFTWARE LICENSE B (Version 1.1 [02/22/2000])	
Mozilla Rhino		Netscape Public License Version 1.1	
NekoHTML		Apache-like (1.1)	
NSIS	1.0j	(see license file)	

Software Name	Version	License type	Source
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
RELAX NG Object Model/Parser		MIT License	
RelaxNGCC		(general permissive)	
RelaxNGCC		version 2003-May-08 of Info-ZIP copyright and license	ftp://ftp.info-zip.org/pub/infozip/license.html
Retroweaver		(general permissive license)	
SAX	v. 2.0.1	Public Domain	
Stax API		BEA License (unique terms)	
Stripper		BSD-like	
UPX		GPL	
W3C XML Conformance Test Suites	v. 20020606	W3C SOFTWARE NOTICE AND LICENSE	
W3C XML Schema Test Collection	v. 1.16.2	W3C SOFTWARE NOTICE AND LICENSE	
W3C XML Schema Test Collection		W3C DOCUMENT NOTICE AND LICENSE	
X Window System		(general permissive license)	
Xalan J2		Apache 2.0	
Xalan, Xerces		Apache 1.1	
XFree86-VidMode Extension		Version 1.1 of Project Licence (BSD-like)	
XML Resolver Library		Apache 2.0	
XML Security		Apache 1.1	
Zlib		(general permissive)	

Resolved Issues

The following table lists the issues resolved in the Polycom DMA 7000 system version 5.0 base release. See "What's New in The Version 5.0.2.1 Release" on page 4 for issues resolved in the subsequent maintenance releases.

Issue ID	Found in Version	Description
DMA-8789		On the Microsoft Active Directory page, the number of characters used for conference room ID generation was limited to 12. That limit has been expanded to 128. Note that the new limit is greater than the maximum dial string allowed by HDX endpoints (100) and twice the maximum length of AD's telephone number field.
DMA-8450	4.0.1	Backup files larger than 2 GB couldn't be uploaded to the system. The maximum value has been increased to 5 GB.
DMA-8283	4.0.3	If a call's bit rate was reduced by endpoint negotiation, the DMA system didn't show the correct bit rate.
DMA-7831	4.0.3	When configuring an external gatekeeper with a prefix, a postliminary script was required to remove the prefix from the dial string that was forwarded to the external gatekeeper.
DMA-7821	4.0.3	If you configured a prefix service for an MCU in the dial plan, you couldn't dial just the prefix to be routed to that MCU. You had to dial something after the prefix value to be routed. This prevented the DMA from routing to the default entry queue on an RMX.
DMA-7812	4.0.3	For gateway calls between some endpoints, the video wasn't displayed on one of the endpoints.
DMA-7774, DMA-7784	4.0, 4.0.3	DMAs integrated to AD prior to upgrading could lose their connection to AD as a result of the upgrade to 4.0.3.
DMA-7737	4.0.3	Call Forwarding On Busy didn't work when forwarding to endpoints not known to the DMA and registered to external proxies.
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.
DMA-7632	4.0, 4.0.1, 4.0.2	Territory delete didn't warn about or clean up users assigned to that territory.
DMA-7567	4.0.3	Postliminary script for MCU wasn't saved.
DMA-7548	4.0.3	If "Allow calls to/from rogue endpoints" was enabled, a call to a blocked endpoint in the Internet/VPN site succeeded.
DMA-7466	4.0.3	When the DMA received a call from a SIP proxy and attempted to connect the call to one of its endpoints, if bandwidth management logic rejected the call after the dialed endpoint responded with a SIP 200 OK message (when the line went off-hook), the DMA terminated the call to that endpoint but not to the calling leg. The calling leg sent 200 OK messages until timeout (less than 30 seconds), and only then did the call fail and resources get properly cleaned up.
DMA-7436	4.0.3	When the primary cluster for a territory was changed, there was no warning dialog explaining that endpoints that were registered would become inactive until they re-registered.
DMA-7418	4.0.3	Deselecting the "Allow calls to/from rogue endpoints" option prevented calls to endpoints in the configured site topology that were not registered to the DMA, even when the endpoints were registered to a neighbored gatekeeper or SIP peer and the neighboring or peering dial rule was used to route the call.
DMA-7369	4.0.2	Calls failed 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.

Issue ID	Found in Version	Description
DMA-7297	4.0.2	After upgrading a DMA system 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.
DMA-7176	4.0.2	Some calls from HDX endpoints using the DMA system as a gateway to Lync clients failed (Ms-client-diagnostics: 52001; reason= "Client side general processing error.").
DMA-7073	4.0.1	SIP endpoints remained listed as inactive (although actually active) after a territory failover.
DMA-6598	4.0	If a two-server cluster was configured without using the USB stick (the alternate procedure in the *Getting Started Guide*), but Server 2 was running while Server 1 was being configured, the two servers could end up not synchronized and not clustered. This left the system in an unusable state.
DMA-6469 DMA-6472	4.0	In a SIP to H.323 call through the DMA system's gateway, the H.323 endpoint transmitted video in H.263 CIF at bit rates up to 6144 kbps.
DMA- 2027	2.3	SIP TLS calls to an older HDX endpoint failed if they traversed two or more DMA clusters.
DMA-1877	2.2	When a call from a VSX endpoint failed over from an RMX MCU to a Codian MCU that hadn't been appropriately configured, the call had no audio.
DMA-1534	2.0	Tandberg and Cisco gatekeepers: Only one DMA server registered with the Tandberg and Cisco GKs. Issue made obsolete by Call Server.

Known Issues

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

Issue ID	Found in Version	Description	Workaround
DMA-9971	5.0.1	The DMA MIB couldn't be loaded into a Zenoss 3.2.1 network manager.	Download the MIB and in a text editor make the following changes in the IMPORTS section: • Add these two lines: TRAP-TYPE FROM RFC-1215 • Change the line ::= { polycom 13 } to ::= { enterprises 13885 } Save the changes and load the modified file into the Zenoss 3.2.1 network manager.
DMA-9361	5.0.1	In a superclustered environment, some call events may appear out of order on the Call Events tab of the Call Details dialog box.	
DMA-9325	5.0	On the Call History page, records found by a dial string search may have an empty End Time field even though they have an end time.	

Issue ID	Found in Version	Description	Workaround
DMA-9324	5.0	When a rogue or neighbored call traverses two or more DMA clusters within one second, the call records from the clusters aren't always merged correctly, leading to inconsistent Call History information. **Note:** This problem is resolved for callers managed by one of the clusters in the supercluster.	
DMA-9268	5.0	The DMA system uses port 8989 for supercluster replication, but that port isn't included in the "System Port Usage" list in the online help and Operations Guide.	In order to form a supercluster, you must make sure that the network firewall doesn't block port 8989.
DMA-9142	5.0	An API client attempted to start a conference, and the DMA system returned a 503 error indicating insufficient MCU resources when that wasn't the case.	
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.	
DMA-9139		The DMA system doesn't support CMA or RealPresence Resource Manager address book services for H.320 devices.	
DMA-9131		When a call forwarding loop involves an endpoint with multiple lines, the call keeps ringing that endpoint and can't be ended by the calling endpoint.	
DMA-9128	5.0	The Users list can't be sorted on the Associated Endpoints column.	
DMA-9123	5.0	A call forwarding loop may cause Adobe Flash to crash.	In a new browser window, log back in.
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-9115	4.0.3 P1	The DMA system creates an active call entry for an OCS chat INVITE.	
DMA-9098	4.0.3	MCUs added to a DMA system prior to version 4.0 are deleted 30 days after the system is upgraded to version 4.0 or later.	After upgrading, edit each MCU. In the Edit MCU dialog box, select Permanent to prevent the MCU's registration with the Call Server from ever expiring.
DMA-9085	5.0	On the Resource Manager Server page, Model is "CMA" for a RealPresence Resource Manager system.	
DMA-9080	4.0.3 P1 HF1	Network Settings: If Auto-negotiation is turned off and Speed set manually, after rebooting, Auto-negotiation is back on.	
DMA-9027	4.0.3	If SIP device authentication is enabled, it can be turned off for a specific endpoint, but not for a SIP peer.	

Issue ID	Found in Version	Description	Workaround
DMA-9010	5.0	Sony PCS-1 and PCS-G50 endpoints are unable to remain connected in H.323 calls when they're registered to the DMA gatekeeper.	
DMA-8975	5.0	Attempt to edit an MCU with active calls, and the system displays an error message stating that it "cannot be deleted when there are either active calls or conferences."	
DMA-8969	5.0.1	On the Call Info tab of the Call Details dialog, the originator of the call may be misidentified.	The originator of the call is correctly identified on the Call Events tab of the Call Details dialog.
DMA-8952	5.0	When multiple API clients are creating users, a concurrent sorted search can fail.	
DMA-8940	5.0	The DMA system should drop a Bronze call if necessary to free up bandwidth for a Gold call. But if the calls are to the same VMR, it fails to do so.	
DMA-8936, 8937	5.0	On point-to-point calls between Interactive Telepresence (ITP) systems, the ITP codecs (endpoints) may connect at different bit rates.	
DMA-8912	4.0.3 P1	Under certain circumstances the status between local DMA clusters is incorrect even though the servers continue to function properly.	
DMA-8906	4.0.3 P1	DMA UI allows host name and domain name entries of invalid length.	Limit host name and domain name to a combined maximum of 64 characters.
DMA-8904	5.0	On dial-outs from a VMR to an endpoint, the system incorrectly records the originator of the call as the endpoint (affects Active Calls, Call History, and CDRs).	
DMA-8885	5.0	When a caller with a higher quality of service (QoS) setting dials into a conference and there isn't sufficient bandwidth, lower QoS calls are correctly dropped, but the higher QoS caller must redial in order to get into the conference.	
DMA-8875	5.0	When a conference uses a custom conference template with auto layout enabled, auto layout sometimes doesn't work.	
DMA-8869	5.0.1	When a VMR call that traverses two DMA clusters and is pinned to the Active Calls screen ends, its Destination field reverts from the MCU name to the dialed digits.	
DMA-8854	5.0.1	On the Call Events tab of the Call Details dialog box, some call events for SIP VMR calls may appear out of order.	

Issue ID	Found in Version	Description	Workaround
DMA-8836	5.0	Integrating the DMA system with a RealPresence Resource Manager doesn't automatically integrate the RealPresence Resource Manager with the DMA system (that is, connect it to the DMA system's API).	On the RealPresence Resource Manager, integrate it with the DMA system. The integration of the DMA system back to the RealPresence Resource Manager is automatically created.
DMA-8818	5.0	At certain display resolutions and/or browser window sizes, some DMA dialog boxes may be cut off.	Use at least the minimum supported display resolution (1280x1024) and maximize the browser window.
DMA-8815	5.0	When an RMX MCU is in dual stack (IPv4 + IPv6) mode, the DMA system attempts to respond to it via IPv6 even though it's in IPv4-only mode.	
DMA-8791	5.0	When an RMX MCU registers with Call Server, its internal 172 address may appear in the list of media IP addresses.	The DMA system receives this IP address from the RMX MCU and simply reports it.
DMA-8715	5.0	Removing a cluster from the supercluster may cause Adobe Flash to crash.	In a new browser window, log back in.
DMA-8675	5.0	On calls to VMR, DMA system shows different requested and final bit rates than the MCU and endpoints show.	
DMA-8601	5.0	Downloading call detail records (CDRs) can take a long time (> 2 minutes) when there are many CDRs in the system.	
DMA-8578	5.0	When the DMA system and an RMX MCU were both in maximum security mode and the RMX MCU was registered with the DMA gatekeeper, the MCU couldn't securely connect to the DMA system.	
DMA-8567	5.0	After switching from IPv4+IPv6 to IPv4 only, it may not be possible to download logs.	Reboot the system and try again.
DMA-8542	5.0	After upgrading a two-server cluster to 5.0, the Dashboard may show one of the servers not available.	Reboot the unavailable server.
DMA-8514	5.0	Active Calls and Call History may show different bit rates for same call.	
DMA-8489	5.0	Under certain conditions, the host portion of an endpoint's SIP URI may be altered by the internal DMA call flow processing, and the call history record contains the altered host.	
DMA-8186	4.0.3	Calls from the 32-bit version of the Lync 2010 client to a DMA VMR hosted on an RMX 1500 MCU don't receive video.	Use an RMX 2000 or 4000 MCU, or upgrade the user to the 64-bit version of Lync 2010.
DMA-7981	5.0	In the call CDRs of VMR calls, the userRole field for participants is often null.	
DMA-7834	4.0, 4.0.3	In rare instances, an upgrade or rollback can result in not being able to log in to the GUI as any user.	Reboot the DMA.

Issue ID	Found in Version	Description	Workaround
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 do not.	Retry the integration until it succeeds. To avoid this form of cache loading failure, integrate to an AD server that has sufficient performance.
DMA-7695	4.0.2	High failure rate on SIP registrations from RMX MCUs.	
DMA-7636	3.0 P1, 4.0, 4.0.1, 4.0.2	M100 software endpoint version 1.0 cannot successfully make calls to or receive calls from Lync users through DMA when DMA/Lync integration is enabled.	
DMA-7614	4.0.2	When conference management has failed over to the backup cluster for a territory, and the primary cluster is brought back online, there is a period of time (approximately 1 second for every 3000 enterprise users) when new calls can't join conferences in the territory.	
DMA-7541	4.0.2	Deleting the territory used for Active Directory integration is incorrectly permitted.	If you need to delete the default territory, create a new territory and associate it with the AD integration prior to deleting the territory associated with AD integration.
DMA-7223, DMA-7230	4.0.2	Due to a limitation of the Microsoft Lync client on Apple computers, video is not supported on calls to or from Lync clients for the Macintosh.	Voice-only calls are supported, as long as the endpoints involved support the G.711 codec.
DMA-7168	4.0.1	HDX or Lync SIP calls to encrypted virtual meeting rooms (VMRs) via a virtual entry queue (VEQ) are hooked when being transferred to the VMR.	Use an unencrypted VMR.
DMA-7131	4.0.1	A VBP allows endpoints on external networks to register through it to a LAN-side GK (DMA), proxying H.323 events from the public network to the internal network. The VBP sends all H.323 traffic from the same call signaling address and endpoint identifier (it uses the endpoint identifier of the last endpoint that successfully registered to the gatekeeper to refresh all its endpoint registrations). As a result, DMA displays all VBP calls as having the same endpoint information as the device that sent the successful registration to the DMA and was assigned the endpoint identifier in the RCF.	

Issue ID	Found in Version	Description	Workaround
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-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-6494	4.0	When a Cisco endpoint registered to the DMA system has TLS verification enabled, encrypted calls to the endpoint fail.	On the endpoint, turn off TLS verification.
DMA-6482	4.0	If the DMA system has a large number (over 100,000) of calls in its call history, upgrading to v4.0 can take over one hour.	In advance of the upgrade, on the History Retention Settings page, reduce the number of call history records to retain.
DMA-6480	4.0	In a SIP to H.323 or H.323 to SIP call with content through the DMA system's gateway, neither endpoint receives content-related statistics.	
DMA-6459	4.0	A conference passcode created on the DMA system may not conform to the passcode rules enforced by the MCU hosting the conference, causing calls to fail.	Make sure that the passcodes created on the DMA system meet the requirements of the MCUs that the system uses.
DMA-6103	3.0	In an environment with both a DMA system and a Cisco Unified Conference Manager (CUCM), video path problems were encountered if certain endpoints (Cisco 9971, Polycom HDX9002, and Polycom V500) were registered to the CUCM.	Register the endpoints to the DMA system.
DMA-6101	4.0	Under some circumstances, it may become impossible to log into one server of a two-server cluster because of a heartbeat failure stemming from a time disparity between the two servers.	Use NTP to synchronize the time on both servers and reboot the servers.
DMA-6033	4.0	On the Conference Settings page, the DMA system's default maximum bit rate setting defaults to 2048, and that limit applies to both conference and non-conference (Call Server) calls. This may cause calls to or from Immersive Telepresence (ITP) systems requiring higher bit rates to fail.	On the Conference Settings page, change the default maximum bit rate setting to Unlimited.

Issue ID	Found in Version	Description	Workaround
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-5313	3.0	The Property Changes tab of the Call Details dialog box sometimes contains entries with duplicate sequence numbers.	
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- 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- 4604	3.0	Calling a SIP endpoint registered to a Broadsoft Network Server from a SIP endpoint registered to the DMA system may result in a calling loop.	
DMA- 3750	2.3, 3.0	In a two-server cluster, under certain adverse system and/or network conditions on either server, the virtual address may move between servers when it shouldn't. This could result in the disconnection of both SIP calls and H.323 calls.	The system automatically recovers, so disconnected callers can dial back in a short time later (1 - 10 seconds).
DMA- 3745	2.3	It's possible to log into Server 1 of a two-server cluster and initiate an upgrade while Server 2 is still booting, causing the two servers to be out of sync and running different versions.	Do not perform upgrade, rollback, or system reconfiguration operations without both servers being up and active.
DMA- 3426	2.3, 3.0	If a DMA cluster is the primary or backup for a territory, it can't be removed from the supercluster via the management interface until the territory responsibilities are removed. But there is no warning that territory responsibilities need to be corrected afterward.	After removing a cluster from a supercluster, always check and correct territory responsibilities.
DMA- 3390	2.3	If a DMA cluster is the primary or backup for a territory, it 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.

Issue ID	Found in Version	Description	Workaround
DMA- 2797	2.3	Some Sony endpoints that register with the DMA system become unregistered after five minutes.	
DMA- 2717	2.2	If a "spoke" MCU with a cascade link to the "hub" MCU is registered with an unavailable GK, callers on the two MCUs are isolated from each other. No indication in GUI or logs.	Do one of the following: 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- 2411	2.2	Calls from endpoints registered to a Tandberg VCS GK don't include the IP address of the endpoint, so the DMA system can't determine the site to which the endpoint belongs. For cascaded conferences, the call ends up either in the hub conference or, if the VCS GK is in a defined site, in a spoke conference near the VCS GK.	Place the IP address of the VCS into a site near the bridges to be used for spokes.
DMA- 2362	2.3	In some situations, SIP calls from an RMX to an HDX join with only video - no audio.	
DMA- 2014	2.3	Polycom HDX and PVX endpoints don't support failover of SIP registrations.	
DMA- 1939, 1941, 1948	2.3	H.323 calls using dial strings of the form <IP Address>##<Alias> sometimes fail.	The DMA supports such dial strings for both inbound and outbound calls, routing them to the specified gatekeeper or MCU IP address. Interpretation of the alias depends on the destination gatekeeper or MCU. Use of this feature is not recommended, however, because support for it varies significantly among different kinds of endpoints.
DMA-2109	2.3	Polycom V500 endpoints don't support failover of SIP registrations.	
DMA-1691	2.0	Calls from Tandberg 6000 E and 6000 B endpoints are unable to join a DMA meeting.	
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.

Where to Get the Latest Product Information

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

Welcome to Polycom® Distributed Media Application™ (DMA™) 7000
(Software Version 5.0)

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