

# Release Notes

## Polycom® Distributed Media Application™ 7000 System, Version 4.0.2 Release



Polycom® announces the release of its Polycom® Distributed Media Application™ (DMA™) 7000 System, version 4.0.2. This document provides the latest information about this release.

### Topics

---

Introducing the Polycom DMA™ 7000 System.....	2
What's New in the Version 4.0.2 Release .....	3
What's New in the Version 4.0 Release .....	4
The Consequences of Enabling Maximum Security Mode.....	6
System Requirements.....	8
Installation and Upgrade Notes .....	8
Polycom Solution Support .....	9
Interoperability .....	9
Open Source Software .....	12
Resolved Issues.....	17
Known Issues .....	17
Where to Get the Latest Product Information .....	21
END USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE .....	22

### Copyright Information

© 2012 Polycom, Inc. All rights reserved.

3725-76300-001Q (02/2012)

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

### Trademark Information



Polycom®, the Polycom "Triangles" logo, and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common-law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.



Java is a registered trademark of Oracle America, Inc., and/or its affiliates.

## 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 22.

### Conference Manager

- ❑ Provides a highly reliable and scalable multipoint conferencing solution that distributes voice and video calls across multiple media servers (MCUs), creating a single seamless resource pool. The system essentially behaves like a single large MCU, which greatly simplifies video conferencing resource management and improves efficiency.
- ❑ Supports up to 64 MCUs. MCUs can be added on the fly without impacting end users and without requiring re-provisioning.
- ❑ Can be configured as a two-node cluster, providing a highly reliable system with no single point of failure.

### Call Server

- ❑ Provides complete endpoint registration and call routing services for both H.323 and SIP protocols. It also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to begin transitioning to SIP in a gradual, orderly, and cost-effective manner.
- ❑ Provides bandwidth management, and can be integrated with a Juniper Networks Session and Resource Control Module (SRC) to provide bandwidth assurance services.
- ❑ Comes with a default dial plan that covers many common scenarios, but which can easily be modified.
- ❑ Can be deployed as a *supercluster* of up to five geographically dispersed, but centrally managed, Polycom DMA system clusters (two-node or single-server) to provide even greater reliability, geographic redundancy, and better network traffic management. Up to three of the clusters can have Conference Manager enabled.

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

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

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

The Polycom DMA 7000 system also:

- ❑ Integrates with Microsoft Active Directory, automating the task of provisioning users for video conferencing. Combined with its advanced resource management, this makes ad hoc video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.
- ❑ Integrates with Microsoft Exchange Server, enabling users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.
- ❑ Integrates with a Polycom CMA 5000 system to obtain site topology and user-to-device association data.

## What's New in the Version 4.0.2 Release

The version 4.0.2 release fixes a number of issues found in the version 4.0 base release or version 4.0.1 release and replaces those releases.

### Issues Resolved in Version 4.0.2

The following table lists the issues resolved in this release.

Issue ID	Description
DMA-5961	When a SIP VVX1500 endpoint calls an H.323 VVX1500 endpoint, and the endpoints are using the H.263 video codec, the H.323 endpoint doesn't receive video.
DMA-6532	When an H.323 HDX endpoint calls a SIP VVX endpoint, and the endpoints are using the H.264 video codec, the H.323 endpoint doesn't receive video.
DMA-6553	In a Microsoft Lync environment, H.323 endpoints using the DMA system as a gateway are unable to connect to Lync clients. Note: The Lync user must click the <b>Share my video</b> button for the call to complete negotiation. Also, see DMA-7176 in the "Known Issues" list on page 17 for a related problem and its workaround.
DMA-6629	When an HDX endpoint using H.323 calls a SIP HDX endpoint via the DMA gateway, and the endpoints are using 1080p, the H.323 endpoint doesn't receive video.
DMA-6862	When restoring from a backup, one of the datastore processes may become stuck.
DMA-6964	Bad performance of H.323 registration.
DMA-6968	Some configuration lost during upgrade to version 4.0.1.
DMA-6978	DMA outbound registration From: field doesn't comply with mandatory parameters according to RFC3261.
DMA-6993	Dashboard: On "Call Server Active Calls" pod, the TOTAL numbers are greater than the sum of all the nodes.
DMA-7017	Unable to register on Exchange with error: "Exchange Authentication failed" if NTLM v2 is forced.
DMA-7019	Call from H.323 EP which registered on CMA to SIP EP registered on DMA failed.
DMA-7021	Performance issues when a system is swarmed by registration requests on start-up.
DMA-7041	DMA does not maintain configuration and EP provisioning data after upgrade.
DMA-7088	When importing CMA site topology from CMA, DMA should adjust the values to reconcile the difference bandwidth calculations.
DMA-7115	DMA v4.0.1 GA, node 2 got stuck when becoming the primary node.
DMA-7119	DMA cluster lost unexpectedly its call licenses (600 > 10)
DMA-7167	In some rare instances, data corruption may occur during upgrade.
DMA-7184	Leaking RAS transactions cause the GK to stop accepting registrations.
DMA-7187	When a certificate is loaded with a DirName SAN, the GUI can no longer access the certificates.
DMA-7188	NonRepudiation bit in CSR causes some CAs to not sign cert.

## Issues Resolved in Version 4.0.1

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

Issue ID	Description
DMA-6272	When the DMA system attempts to register with an external SIP device or server, it doesn't present its credentials if challenged.
DMA-6408	When a territory's backup cluster is serving as gatekeeper and the primary cluster restarts, the backup cluster sends URQs telling registered devices to re-register with the primary cluster before the primary cluster is ready to accept registrations.
DMA-6412	When a territory's primary cluster was gracefully shut down, the backup cluster erroneously rejected lightweight registration requests (LWRRQs) from devices registered with the primary cluster. The backup cluster allowed devices to register only after they sent a full registration request.
DMA-6525	When a territory's primary cluster comes back into service, it sends disengage requests (DRQs) to endpoints connected to an RMX conference room despite being in direct, not routed, mode.
DMA-6611	When embedded DNS is enabled or its domain field modified, the DNS service doesn't start or restart until the system is rebooted.
DMA-6645	When it sends H.323 Annex O dial strings to a Tandberg VCS gatekeeper, the DMA system includes only the user part of the URL in the request. The Tandberg VCS expects the whole URL, and the call fails.
DMA-6662	Alerts and daily statistics were not updating because the console service was blocked from starting due to socket bind issues.
DMA-6668	Calls from unregistered endpoints to endpoints registered to a neighbored gatekeeper fail the "Resolve to external gatekeeper" dial rule.
DMA-6699	When a territory's primary cluster receives an LWRRQ from an HDX endpoint, it erroneously rejects it (rejectReason: fullRegistrationRequired). The endpoint then sends an RRQ to the backup cluster.
DMA-6716	The DMA system improperly handles multiple devices registering with the same SIP user name, instead of letting the last endpoint to register with a particular name prevail.
DMA-6726	When a territory's primary cluster reboots, it doesn't send URQs to endpoints that are in a call.
DMA-6737	Calls from a CTS system to an RMX MCU through the DMA system fail after a few seconds.
DMA-6751	The DMA system improperly handles some special characters in Active Directory group names, causing a cache load failure when a group name contains special characters.
DMA-6761	When a territory's primary cluster comes back into service, the backup cluster sends URQs to endpoints and MCUs in a call.

## What's New in the Version 4.0 Release

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

### ❑ Removal of legacy signaling mode

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



---

*Upgrading a system without Call Server functionality to this version is a significant change that must be fully understood and planned for. It requires changes to your existing gatekeeper(s) and dial plan. Don't upgrade until you're prepared to use the Polycom DMA system as an H.323 gatekeeper and/or SIP registrar/proxy. See "Existing System Upgrade" on page 8.*

---

❑ Registration with SIP peers

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

❑ Gatekeeper support for IPv6

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

❑ Registration control

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

❑ New **Dashboard** panes

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

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

The legacy dashboard has been removed.

❑ History of system alerts

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

❑ Maximum security mode

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

Enabling the **Maximum security** setting is *irreversible* and has significant consequences. See "The Consequences of Enabling Maximum Security Mode" on page 6 for a complete list of the special security features enabled by this setting and the features that aren't supported in this mode.

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

❑ Support for new RMX conference settings

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

- **H.264 high profile** – Enables conferences in video switching mode (VSW) on RMX v7.6 MCUs with MPMx cards to use Polycom’s bandwidth-conserving H.264 High Profile codec (previously supported only in continuous presence mode). All endpoints in such a conference must support High Profile. Endpoints not connecting at the conference’s exact line rate and resolution are connected in audio-only mode.
- **TIP compatibility** – Enables RMX v7.6 MCUs with MPMx cards to natively inter-operate with Cisco TelePresence® Systems (CTS), using Cisco’s proprietary Telepresence Interoperability Protocol (TIP). Conferences can include both endpoints that don’t support TIP and CTS endpoints.

❑ SIP interoperability enhancements

This release incorporates a number of enhancements in its SIP signaling functionality that improve interoperability with third-party products. These enhancements include support for:

- Cisco TIP
- Microsoft OCS CAC-14
- Avaya
- Broadsoft
- Siemens

## The Consequences of Enabling Maximum Security Mode

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

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

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

Similarly, an Active Directory server certificate often specifies only the FQDN. So, in the Polycom DMA system, identify the enterprise directory by FQDN, not by IP address.

- ❑ SIP signaling is not supported.

- ❑ The Polycom DMA system can't be integrated with Microsoft Exchange Server and doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.
- ❑ Integration with a Polycom CMA system is not supported.
- ❑ Superclustering is not supported.
- ❑ On the **Banner** page, **Enable login banner** is selected and can't be disabled.
- ❑ On the **Login Sessions** page, the **Terminate Session** action is not available.
- ❑ On the **Tools** menu, **Top** is removed.
- ❑ In the **Add User** and **Edit User** dialog boxes, conference and chairperson passwords are obscured.
- ❑ After **Maximum security** is enabled, users must change their passwords.
- ❑ If the system is integrated with Microsoft Active Directory, only one local user can have the Administrator role, and no local users can have the Provisioner or Auditor role.

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

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

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

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

- ❑ Local user passwords have stricter limits and constraints (each is set to the noted default if below that level when you enable the **Maximum security** setting):
  - Minimum length is 15-30 characters (default is 15).
  - Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).
  - Maximum number of consecutive repeated characters is 1-4 (default is 2).
  - Number of previous passwords that a user may not re-use is 8-16 (default is 10).
  - Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).
  - Password may not contain the user name or its reverse.
  - Maximum password age is 30-180 days (default is 60).
  - Minimum password age is 1-30 days (default is 1).
- ❑ Other configuration settings have stricter limits and constraints (each is set to the noted default if below that level when you enable the **Maximum security** setting).

Session configuration limits:

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

- Session timeout is 5-60 minutes (default is 10).

Local account configuration limits:

- Local user account is locked after 2-10 failed logins (default is 3) due to invalid password within 1-24 hours (default is 1).
- Locked account remains locked either until unlocked by an administrator (the default) or for a duration of 1-480 minutes.
- ❑ Software build information is not displayed anywhere in the interface.
- ❑ You can't restore a backup made before the **Maximum security** setting was enabled.
- ❑ File uploads may fail when using the Mozilla Firefox browser unless the proper steps have been taken. See the *Polycom DMA 7000 System Deployment Guide for Maximum Security Environments*, the *Polycom DMA 7000 System Operations Guide*, or the online help.

## System Requirements

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

## Installation and Upgrade Notes

### New System Installation

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

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

### Existing System Upgrade

Polycom DMA systems running versions 2.3 or 3.0 (with or without service packs) can be upgraded to version 4.0.2. This upgrade requires a new license key after the upgrade. Systems running version 4.0.0 can be upgraded without needing a new license key.

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

Customers upgrading a version 2.3 system, or a version 3.0 system that has Call Server disabled (the **Legacy signaling mode** option), must be prepared for the significant signaling changes introduced by the Call Server function (see “Call Server” on page 2 and “What’s New in the Version 4.0 Release” on page 4).

When such a system is upgraded to version 4.0, the upgrade process adds any gatekeeper to which it was previously registered to the list of neighbor gatekeepers. The neighbor gatekeeper(s) must then be reconfigured to treat the Polycom DMA system as a trusted neighbor and route calls to it. For a Polycom CMA system, this requires the following steps:

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

**Pattern Type:** Prefix

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

**Action:** Route to a trusted neighbor

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

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

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

## Polycom Solution Support

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

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

## Interoperability

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

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

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

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



*Note: The Automatic Password Generation feature, introduced in RMX version 7.0.2, is not compatible with the Polycom DMA system. On Polycom RMX MCUs to be used with the Polycom DMA system, disable this feature by setting the system flags NUMERIC\_CONF\_PASS\_DEFAULT\_LEN and NUMERIC\_CHAIR\_PASS\_DEFAULT\_LEN both to 0 (zero).*

### IRQ/IRR Handling

The Polycom DMA gatekeeper sends an InfoRequest (IRQ) message to an endpoint when it first registers with the gatekeeper. If the endpoint responds with an InfoRequestResonse (IRR) to the initial request, the DMA gatekeeper marks that the endpoint has the ability to process IRQs. For endpoints that DMA has determined support IRQs, DMA sends an IRQ message at the interval specified in the IRQ sending interval (seconds) on the **Admin->Call Server->Call Server Settings** page. If the endpoint responds to that IRQ with an IRR indicating invalid call (old VVX versions prior to 4.0.1; see EBCS-14) or no call information (old versions of the m100), the DMA gatekeeper terminates the call. This may also be the case with other endpoints that improperly handle IRQ/IRR.

### Device Version Compatibility

The following list is not a complete inventory of compatible equipment. It simply indicates the products that have been tested for compatibility with the Polycom DMA system version 4.0 release.

Device	Version	Notes
Acme Packet Session Border Controller		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
Aethra X3	12.1.19	
Aethra X7	12.1.7	
Avaya 1000 series endpoints		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
Avaya Aura Communication Manager (H.323)		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
Avaya Aura Session Manager		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
Avaya Aura System Manager		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
Avaya One-X Communicator		Please consult the Polycom UC Deployment Guide for Avaya Aura Environments for a list of supported versions and interoperability scenarios.
BroadSoft BroadWorks Application Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.

Device	Version	Notes
BroadSoft BroadWorks Media Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
BroadSoft BroadWorks Network Server		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
Cisco (Tandberg) 150 MXP	L6.0, L6.1	
Cisco (Tandberg) 6000 B Series	EB10.3	
Cisco (Tandberg) 6000 E Series	E5.3	
Cisco (Tandberg) C20	4.1.1, 4.1.2	
Cisco (Tandberg) C90	4.1.1, 4.1.2	
Cisco (Tandberg) E20	4.0.0	
Cisco (Tandberg) EX90	4.1.1, 4.1.2	
Cisco (Tandberg) GK	N6.1	
Cisco (Tandberg) MCU 4210	4.0, 4.1, 4.2	
Cisco (Tandberg) MCU 4505	4.0, 4.1, 4.2	
Cisco (Tandberg) MXP	F9.0, F9.1	
Cisco 3745 GK	12.4	
Cisco IP Communicator		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Cisco Unified Communication Manager		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Cisco Unified IP Phones		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Cisco Unified Personal Communicator		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Cisco Unified Video Advantage		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Cisco Unified Videoconferencing 5230		Please consult the Polycom UC Deployment Guide for Cisco Environments for a list of supported versions and interoperability scenarios.
Edgewater EdgeMarc		Please consult the Polycom UC Deployment Guide for BroadSoft BroadWorks Environments for a list of supported versions and interoperability scenarios.
IBM Sametime Connect Client		Please consult the Polycom UC Deployment Guide for IBM Lotus Sametime Environments for a list of supported versions and interoperability scenarios.
IBM Sametime Media Manager Server		Please consult the Polycom UC Deployment Guide for IBM Lotus Sametime Environments for a list of supported versions and interoperability scenarios.
Lifesize Room	4.7.17(1)	
Lifesize Team 220	4.8.0(59)	
Microsoft Lync		Please consult the Polycom UC Deployment Guide for Microsoft Environments for a list of supported versions and interoperability scenarios.
Polycom CMA	5.x, 6.x	
Polycom CMAD	5.x	
Polycom DST B5	2.0	
Polycom DST K60	2.0.1	

Device	Version	Notes
Polycom FX	6.0.5	
Polycom HDX	2.x.y, 3.x.y	
Polycom iPower 9000	6.2.0	
Polycom ITP (RPX, APX, OTX)	3.0.3	
Polycom m100	1.0	
Polycom MGC 50+	9.0.4.3	
Polycom PathNavigator	7.00.12	
Polycom PVX	8.0.4, 8.0.16	
Polycom QDX4000	4.0.1.1	
Polycom RMX1000	2.1	
Polycom RMX1500, 2000, 4000	6.x, 7.x	
Polycom SE200	3.00.07	
Polycom SoundPoint 601/650 SIP	3.3.1	
Polycom V500	9.0.6.1	
Polycom VS	7.5.4	
Polycom VSX	9.0.6.1	
Polycom VVX1500	4.0.1	Versions prior to 4.0.1 are not compatible due to a VVX defect. See DMA-6749 in the "Known Issues" list on page 17.
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	

## 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.

<b>Software</b>	<b>Version</b>	<b>License</b>	<b>Link</b>
Axis	1.4.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
bsf	2.3.0-rc1	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
CentOs	5.6	GPLv2	<a href="https://www.redhat.com/licenses/gpl.html">https://www.redhat.com/licenses/gpl.html</a>
Cluster-glue	1.0.5	GPLv2	<a href="http://www.gnu.org/licenses/old-licenses/gpl-2.0.html">http://www.gnu.org/licenses/old-licenses/gpl-2.0.html</a>
commons-beanutils	1.7	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-collections	3.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-configuration	1.5	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-digester	1.6	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-discovery	0.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-fileupload	1.2.1	Apache License, Version 2	<a href="http://commons.apache.org/fileupload/license.html">http://commons.apache.org/fileupload/license.html</a>
commons-httpclient	3.0.1	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-io	1.4	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-jexl	1.0	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-jxpath	1.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-lang	2.3	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-logging	1.0.4	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
commons-pool	1.3	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
corosync	1.2.5	BSD	<a href="http://opensource.org/licenses/bsd-license.php">http://opensource.org/licenses/bsd-license.php</a>
dom4j	1.5.2	BSD-style	<a href="http://www.dom4j.org/license.html">http://www.dom4j.org/license.html</a>
drools	4.0.0	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
Hibernate Annotations	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Hibernate (core)	3.2.4 SP 1	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Hsqldb	2.0.1-rc1	BSD-style	<a href="http://hsqldb.org/web/hsqldbLicense.html">http://hsqldb.org/web/hsqldbLicense.html</a>
JAF	1.1	Sun	<a href="http://download.oracle.com/otn-pub/java/licenses/jaf-1.1-fr-oth-JPR_license_1.html">http://download.oracle.com/otn-pub/java/licenses/jaf-1.1-fr-oth-JPR_license_1.html</a>
jamon	2.2	BSD-style	<a href="http://jamonapi.sourceforge.net/#JAMonLicense">http://jamonapi.sourceforge.net/#JAMonLicense</a>
Java JRE	1.6.0.20	Sun Microsystems, Binary Code license (BCL)	<a href="http://www.java.com/en/download/license.jsp">http://www.java.com/en/download/license.jsp</a>

Software	Version	License	Link
JavaMail	1.4	Sun	<a href="http://download.oracle.com/otn-pub/java/licenses/javamail-1.4-oth-JPR_license_1.html">http://download.oracle.com/otn-pub/java/licenses/javamail-1.4-oth-JPR_license_1.html</a>
JBOSS AS	4.2.1 GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-aop	1.5.5	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-cache	1.4.1.sp14	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-jaxws	2.0.0.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-jmx	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-remoting	2.2.2.sp1	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jboss-serialization	4.2.1.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
Jgroups	2.4.8.GA	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
jcifs	1.3.2	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
jna	3.0.9 b0	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
joesntp	0.3.4	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
libesntp	1.0.4	LGPLv2.1	<a href="http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html">http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html</a>
libnet	1.1.4		
libxml2	1.2.3	MIT License	<a href="http://www.opensource.org/licenses/mit-license.html">http://www.opensource.org/licenses/mit-license.html</a>
Log4j	1.2.14	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
NSS	Part of Centos distribution	Mozilla Public License v1.1	<a href="http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1">http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1</a>
NSS Tools	Part of Centos distribution	Mozilla Public License v1.1	<a href="http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1">http://www.mozilla.org/projects/security/pki/nss/faq.html#q3.1</a>
NTP	Part of Centos distribution	Open Software License v3.0	<a href="http://www.opensource.org/licenses/http-license.php">http://www.opensource.org/licenses/http-license.php</a>
OpenDS	2.2.0	CDDL	<a href="http://www.opensource.org/licenses/cddl1.php">http://www.opensource.org/licenses/cddl1.php</a>
openSSH	Part of Centos distribution	OpenSSH	<a href="http://www.openssh.org">http://www.openssh.org</a>
openSSL	Part of Centos distribution	OpenSSL	<a href="http://www.openssl.org/source/license.html">http://www.openssl.org/source/license.html</a>
Python	Part of Centos distribution	Python Software Foundation License Version 2	<a href="http://python.org/download/releases/2.6.2/license">http://python.org/download/releases/2.6.2/license</a>
Quartz	1.5.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>

Software	Version	License	Link
Snmp4j	1.10.2	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
sudo	1.7.2p1	ISCL	<a href="https://www.isc.org/software/license">https://www.isc.org/software/license</a>
Xerces2	See JBoss.	Apache License, Version 2	<a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>
OpenFire		Apache License, Version 2	<a href="http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html">http://www.igniterealtime.org/builds/openfire/docs/latest/LICENSE.html</a>
Rhino		Mozilla Public License, v1.1	<a href="http://www.mozilla.org/MPL/MPL-1.1.html">http://www.mozilla.org/MPL/MPL-1.1.html</a> <a href="https://developer.mozilla.org/en/Rhino_License">https://developer.mozilla.org/en/Rhino_License</a>
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.	<a href="http://creativecommons.org/licenses/by-nc-sa/3.0/">http://creativecommons.org/licenses/by-nc-sa/3.0/</a> <a href="http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html">http://www.adobe.com/communities/guidelines/ccplus/commercialcode_plus_permission.html</a>
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 <a href="http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT">http://downloads.polycom.com/Oracle/THIRDPARTYLICENSEREADME.TXT</a>			
CS CodeViewer	v1.0	BSD-like	
Crimson	v1.1.1	Apache 1.1	
Xalan J2		Apache 2.0	
NSIS	1.0j	(see license file)	
IAIK PKCS Wrapper		BSD-like	
Document Object Model (DOM)	v. Level 3	W3C SOFTWARE NOTICE AND LICENSE	
Xalan, Xerces		Apache 1.1	
W3C XML Conformance Test Suites	v. 20020606	W3C SOFTWARE NOTICE AND LICENSE	
W3C XML Schema Test Collection	v. 1.16.2	W3C SOFTWARE NOTICE AND LICENSE	
Mesa 3-D graphics library	v. 5	The core Mesa library is licensed according to the terms of the XFree86 copyright (an MIT-style license). The Mesa source code is licensed under SGI FREE SOFTWARE LICENSE B (Version 1.1 [02/22/2000])	
Byte Code Engineering Library (BCEL)	v. 5	Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
CUP Parser Generator for Java	v. 0.10k	(general permissive license)	

Software	Version	License	Link
JLex: A Lexical Analyzer Generator for Java	v. 1.2.5	(general permissive license)	
SAX	v. 2.0.1	Public Domain	
Cryptix		Cryptix General License	
W3C XML Schema Test Collection		W3C DOCUMENT NOTICE AND LICENSE	
Stax API		BEA License (unique terms)	
X Window System		(general permissive license)	
dom4j v. 1.6		BSD-like	
Retroweaver		(general permissive license)	
Stripper		BSD-like	
libpng official PNG reference library		(general permissive license)	
Libungif – An uncompressed GIF library		(general permissive license)	
Ant		Apache 2.0	
XML Resolver Library		Apache 2.0	
ICU4J		ICU License	
NekoHTML		Apache-like (1.1)	
Jing		(general permissive)	
RelaxNGCC		(general permissive)	
RELAX NG Object Model/Parser		MIT License	
XFree86-VidMode Extension		Version 1.1 of Project Licence (BSD-like)	
RelaxNGCC		version 2003-May-08 of the Info-ZIP copyright and license	<a href="ftp://ftp.info-zip.org/pub/infozip/license.html">ftp://ftp.info-zip.org/pub/infozip/license.html</a>
XML Security		Apache 1.1	
Regexp Regular Expression Package	v. 1.2	Apache 1.1	
Zlib		(general permissive)	
Mozilla Rhino		Netscape Public License Version 1.1	
Apache Derby		Apache 2.0	

Software	Version	License	Link
7-Zip		(see file) Some files are LGPLv2.1; some have the unRAR restriction; some are licensed under AES code license	
UPX		GPL	
LZMA Software Development Kit		Common Public License (CPL)	

## Resolved Issues

The following table lists the issues resolved in the Polycom DMA 7000 system version 4.0 release. See “What’s New in the Version 4.0.2 Release” on page 3 for issues resolved in this maintenance release.

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

## Known Issues

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

Issue ID	Found in Version	Description	Workaround
DMA-1527	2.0	When the DMA system is using a Radvision ECS GK set for routed mode, endpoints are displayed twice on the RMX’s EMA.	Configure the Radvision ECS GK to use direct mode routing.

Issue ID	Found in Version	Description	Workaround
DMA-1534	2.0	Tandberg and Cisco gatekeepers: Only one DMA node registers with the Tandberg and Cisco GKs.	
DMA-1691	2.0	Calls from Tandberg 6000 E and 6000 B endpoints are unable to join a DMA meeting.	
DMA-1877	2.2	When a call from a VSX endpoint fails over from an RMX MCU to a Codian MCU that hasn't been appropriately configured, the call has no audio.	
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- 2014	2.3	Polycom HDX and PVX endpoints don't support failover of SIP registrations.	
DMA- 2027	2.3	SIP TLS calls to an older HDX endpoint fail if they traverse two or more DMA clusters. Older versions of HDX won't accept a new TLS connection from a DMA cluster other than the one to which they're registered.	Configure all endpoints to use UDP or TCP for signaling or upgrade older HDX endpoints to the latest software version.
DMA-2109	2.3	Polycom V500 endpoints don't support failover of SIP registrations.	
DMA- 2362	2.3	In some situations, SIP calls from an RMX to an HDX join with only video - no audio.	
DMA- 2411	2.2	Calls from endpoints registered to a Tandberg VCS GK don't include the IP address of the endpoint, so the DMA system can't determine the site to which the endpoint belongs. For cascaded conferences, the call ends up either in the hub conference or, if the VCS GK is in a defined site, in a spoke conference near the VCS GK.	Place the IP address of the VCS into a site near the bridges to be used for spokes.
DMA- 2717	2.2	If a "spoke" MCU with a cascade link to the "hub" MCU is registered with an unavailable GK, callers on the two MCUs are isolated from each other. No indication in GUI or logs.	Do one of the following: <ul style="list-style-type: none"> <li>• Disable cascading for the conference while the GK is unavailable.</li> <li>• Register the RMX to a working GK.</li> <li>• Busy out the RMX while its GK is unavailable.</li> </ul>
DMA- 2797	2.3	Some Sony endpoints that register with the DMA system become unregistered after five minutes.	
DMA- 3390	2.3	If a DMA cluster is the primary or backup for a territory, it can be removed from the supercluster via the USB Configuration Utility with no warning that territory responsibilities need to be corrected afterward.	After removing a cluster from a supercluster, always check and correct territory responsibilities.

Issue ID	Found in Version	Description	Workaround
DMA- 3426	2.3, 3.0	If a DMA cluster is the primary or backup for a territory, it can't be removed from the supercluster via the management interface until the territory responsibilities are removed. But there is no warning that territory responsibilities need to be corrected afterward.	After removing a cluster from a supercluster, always check and correct territory responsibilities.
DMA- 3745	2.3	It's possible to log into Node 1 of a two-node cluster and initiate an upgrade while Node 2 is still booting, causing the two nodes to be out of sync and running different versions.	Do not perform upgrade, rollback, or system reconfiguration operations without both nodes being up and active.
DMA- 3750	2.3, 3.0	In a two-node cluster, under certain adverse system and/or network conditions on either node, the virtual address may move between nodes 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- 3802	2.3	During a bridge failover in a Microsoft Lync environment, calls from Lync clients may not automatically reconnect, and other SIP calls may take several seconds longer than usual to reconnect.	
DMA- 4604	3.0	Calling a SIP endpoint registered to a Broadsoft Network Server from a SIP endpoint registered to the DMA system may result in a calling loop.	
DMA- 5069	3.0	In a superclustered environment, slight time drifts between clusters may produce CDR records out of order or duplicated. If NTP services are properly configured, the system self-corrects, but by then the CDR data is already committed to the database.	NTP services usually keep clocks synced to the second, but sub-second differences may exist in the CDR ordering. Be aware that event order may not be 100% accurate due to time differences. No loss of functionality or data occurs as a result of this issue.
DMA- 5337	3.0	The DMA system doesn't properly handle SIP signaling from Polycom V-series endpoints with firmware prior to v. 9.0.6 (Feb 02, 2010).	Upgrade the endpoints to v. 9.0.6 or later.
DMA- 5862	3.0	HDX endpoints expect H.323 bandwidth to be reserved in 64 kbps increments, but the DMA system uses smaller increments. The DMA system may, for instance, allocate 498 kbps for a call, and the call will use that. But the endpoint displays 448 (64 * 7).	
DMA-6033	4.0	On the Conference Settings page, the DMA system's default maximum bit rate setting defaults to 2048, and that limit applies to both conference and non-conference (Call Server) calls. This may cause calls to or from interactive 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-6101	4.0	Under some circumstances, it may become impossible to log into one node of a two-server cluster because of a heartbeat failure stemming from a time disparity between the two servers.	Use NTP to synchronize the time on both servers and reboot the servers.
DMA-6103	3.0	In an environment with both a DMA system and a Cisco Unified Conference Manager (CUCM), video path problems were encountered if certain endpoints (Cisco 9971, Polycom HDX9002, and Polycom V500) were registered to the CUCM.	Register the endpoints to the DMA system.
DMA-6459	4.0	A conference passcode created on the DMA system may not conform to the passcode rules enforced by the MCU hosting the conference, causing calls to fail.	Make sure that the passcodes created on the DMA system meet the requirements of the MCUs that the system uses.
DMA-6469 DMA-6472	4.0	In a SIP to H.323 call through the DMA system's gateway, the H.323 endpoint transmits video in H.263 CIF at bit rates up to 6144 kbps.	
DMA-6480	4.0	In a SIP to H.323 or H.323 to SIP call with content through the DMA system's gateway, neither endpoint receives content-related statistics.	
DMA-6482	4.0	If the DMA system has a large number (over 100,000) of calls in its call history, upgrading to v4.0 can take over one hour.	In advance of the upgrade, on the History Retention Settings page, reduce the number of call history records to retain.
DMA-6494	4.0	When a Cisco endpoint registered to the DMA system has TLS verification enabled, encrypted calls to the endpoint fail.	On the endpoint, turn off TLS verification.
DMA-6524	4.0	In a SIP to H.323 or H.323 to SIP call through the DMA system's gateway, Far End Camera Control (FECC) doesn't work on either endpoint.	
DMA-6598	4.0	If a two-node cluster is configured without using the USB stick (the alternate procedure in the <i>Getting Started Guide</i> ), but Node 2 is running while Node 1 is being configured, the two nodes can end up not synchronized and not clustered. This leaves the system in an unusable state.	To avoid this problem, follow the procedure in the <i>Getting Started Guide</i> , which requires that Node 2 not be turned on until Node 1 has been configured, finishes rebooting, and displays <b>DMA Ready</b> on the LCD.  To recover from this problem: <ol style="list-style-type: none"> <li>1. Turn off Node 2.</li> <li>2. Reboot Node 1, and wait for it to finish rebooting and display <b>DMA Ready</b> on the LCD.</li> <li>3. Turn on Node 2. It detects and gets its configuration settings from Node 1 and joins the cluster. When done, both servers' LCDs display <b>DMA Clustered</b>.</li> </ol>

Issue ID	Found in Version	Description	Workaround
DMA-6644	4.0	<p>As required by the H.323 specification, the DMA system treats dial strings of the form "h323:&lt;user&gt;@&lt;domain&gt;" as url-IDs (H.323 Annex O) and dial strings of the form "&lt;user&gt;@&lt;domain&gt;" as email-IDs.</p> <p>Other gatekeepers, such as CMA and VCS, treat dial strings of the form "&lt;user&gt;@&lt;domain&gt;" as url-IDs.</p> <p>The DMA system's different treatment of these dial strings means that calls to non-neighbored external gatekeepers are likely to fail.</p> <p>For compatibility purposes, the DMA should have a configuration option to treat these dial strings as url-IDs.</p>	<p>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:</p> <pre>DIAL_STRING=DIAL_STRING.replace(/^([:@]*)@([^\@]*)/, "h323:\$1@\$2");</pre>
DMA-6749	4.0	The SIP to H.323 GW drops calls involving a VVX endpoint running a version prior to 4.0.1 because the VVX mishandles the IRQ/IRR (EBCS-14).	Upgrade the VVX endpoints to VVX software v.4.0.1.
DMA-7173	4.0.2	In rare instances, the Proximo service restarted unexpectedly.	None. The system generally recovers within 30 seconds.
DMA-7176	4.0.2	Despite the fix for DMA-6553, some calls from HDX endpoints using the DMA system as a gateway to Lync clients fail (Ms-client-diagnostics: 52001; reason="Client side general processing error.").	Have the Lync user call the HDX endpoint.
DMA-7223, DMA-7230, DMA-7231	4.0.2	Due to a limitation of the Microsoft Lync client on Apple computers, the DMA system is only compatible with Microsoft Lync clients running on Windows PCs.	
DMA-7239	4.0.2	If a DMA system is rolled back from v4.0.2 to the initial release of v2.3.0, the system is unable to register to an external gatekeeper.	<p>There are two possible workarounds:</p> <p>(1) Prior to upgrading to v4.0.2, download a backup of the DMA running v2.3. If forced to roll back to v2.3, re-image your system using the v2.3 recovery disk and then apply the backup you made prior to upgrading.</p> <p>(2) Alternatively, after rolling back to v2.3 and detecting that this issue exists, upgrade to v3.0 P1 and then roll back to v2.3. That will resolve this issue.</p>

## 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](http://www.polycom.com/support).

**Welcome to Polycom® Distributed Media Application™ (DMA™) 7000  
(Software Version 4.0)**

**END USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE**

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

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

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

**2. OTHER RIGHTS AND LIMITATIONS.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 6. WARRANTY AND WARRANTY EXCLUSIONS.

6.1 Limited Warranty. Except as otherwise set forth in a Third Party License or in third party license terms set forth below, POLYCOM warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the

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

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

NEITHER POLYCOM NOR ITS SUPPLIERS SHALL BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE SOFTWARE PRODUCT DOES NOT EXIST OR WAS CAUSED BY YOUR OR ANY THIRD PARTY'S MISUSE, NEGLIGENCE, 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.

Polycom, Inc. © 2011. ALL RIGHTS RESERVED.  
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>