Release Notes

Polycom® Distributed Media Application™ (DMA®) 7000 System, Virtual Edition, Version 6.0.3 Release

Polycom® announces the release of its Polycom® Distributed Media Application™ (DMA®) 7000 System, Virtual Edition, version 6.0.3. This document provides the latest information about this release.

Topics

Copyright Information

© 2013 Polycom, Inc. All rights reserved.

3725-76300-001X11 (1/2014)

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 (EULA). The EULA for your version is available on the Polycom Support page for the Polycom DMA 7000 system.

Conference Manager

❑ Provides a highly reliable and scalable multipoint conferencing solution that distributes voice and video calls across multiple media servers (MCUs), creating a single seamless resource pool. The system essentially behaves like a single large MCU, which greatly simplifies video conferencing resource management, improves efficiency, and facilitates ad hoc (reservationless) conferencing.

❑ Supports up to 64 MCUs and 1200 concurrent conference (virtual meeting room, or VMR) calls.

❑ MCUs can be added on the fly without impacting end users and without requiring re-provisioning.

Call Server

❑ Provides complete endpoint registration and call routing services for both H.323 and SIP protocols.

❑ Also serves as a gateway between H.323 and SIP, enabling enterprises with legacy H.323 devices to begin transitioning to the use of SIP in a gradual, orderly, and cost-effective manner.

❑ Provides bandwidth management, including tracking resource usage and controlling excessive resource usage.

❑ Can be integrated with a Juniper Networks Session and Resource Control Module (SRC) that provides bandwidth assurance services.

❑ Comes with a default dial plan that covers many common scenarios, but which can be modified in a simple, but powerful and flexible, way.

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

Clustering and Superclustering

Configurations of the Polycom DMA system, Virtual Edition are similar to the Appliance Edition, but have some important differences.

Superclustering of individual DMA system, Virtual Edition instances is fully supported in a virtual environment. The DMA system, Virtual Edition does not support the same two-server local cluster configuration as the Appliance Edition. However, VMware® vSphere HA may be used to protect against server-level failures.

Polycom recommends use of DMA system superclusters to protect against failure of individual DMA system Virtual Edition instances, and vSphere HA for hardware resiliency. See your VMWare documentation for more information on vSphere HA.

The Polycom DMA system, Virtual Edition, can be deployed as a *supercluster* of up to five geographically dispersed, but centrally managed, single-node DMA systems to provide greater reliability, geographic redundancy, and better network traffic management. Up to three of the systems in a supercluster can have Conference Manager enabled.

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

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

Other Key Features

The Polycom DMA 7000 system also:

❑ Integrates with Microsoft® Active Directory®, automating the task of provisioning users for video conferencing. Combined with its advanced resource management, this makes ad hoc video conferencing on a large scale feasible and efficient, reducing or eliminating the need for conference scheduling.

❑ Integrates with Microsoft Exchange Server, enabling users who install the Polycom Conferencing Add-in for Microsoft Outlook to set up Polycom Conferencing meetings in Outlook.

❑ Integrates with a Polycom RealPresence® Resource Manager or CMA system to obtain site topology and user-to-device association data.

❑ Includes the RealPresence Platform Application Programming Interface (API), which provides programmatic access to the Polycom DMA system for the following:

  ▫ Provisioning

  ▫ Conference control and monitoring

  ▫ Call control and dial-out

  ▫ Billing and usage data retrieval

  ▫ Resource availability queries

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

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

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

❑ SNMP support

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

  The system supports SNMPv3 communications with authentication and privacy.

System Capabilities and Constraints

The following capabilities and constraints apply to the entire supercluster:

- ❑ Number of sites: 500

- ❑ Number of subnets: 5000

- ❑ Number of systems 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 system with Conference Manager enabled, 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 system 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 system:

  - ▫ 500,000 registration history

  - ▫ 2,000,000 registration signaling

  - ▫ 500,000 call history

  - ▫ 200,000 conference history

What's New in the Version 6.0.3 Release

The Polycom DMA system version 6.0.3 is a maintenance release that addresses some issues found since the version 6.0.2.1 release and replaces that release. Version 6.0.3 also brings incremental improvements and slight changes to existing features. The online help and Operations Guide don't include the below information.

Additional Call Detail Record Fields

To help administrators more easily determine chairperson-related information about a call or conference, such as whether a conference required a chairperson or whether a participant joined before the chairperson, version 6.0.3 includes the following additional fields in the call and conference CDRs:

Field	Description
chairPasscode	The configured chairperson passcode for the conference room. Blank if no passcode was configured at the time of the conference.

Field	Description
confRequiresChair	TRUE if the conference template used for the conference has the Conference requires chairperson flag enabled. Otherwise, FALSE.
termConfAfterChairDrops	TRUE if the conference template used for the conference has the Terminate conference after chairperson drops flag enabled. Otherwise, FALSE.
chairJoinTime	The time the first chairperson joined the conference. If no chairperson joined the conference until after the call ended, this may be blank.

Changes to Unauthorized Call Dial Rule Functionality

This release changes existing dial rule behavior on the **Admin > Call Server > Dial Rules** page. Prior to version 6.0.3, the actions available to a dial rule for unauthorized calls were restricted to:

> ➢ **Resolve to external SIP peer**

> ➢ **Resolve to conference room ID**

> ➢ **Resolve to virtual entry queue**

With version 6.0.3 and later, the actions available to dial rules for unauthorized calls are unrestricted.

Issues Resolved in Version 6.0.3

The following table lists the issues resolved in version 6.0.3.

Issue ID	Found in Version	Description
DMA-12225	6.0.2 HF1	When an MCU was disconnected and reconnected to the DMA system, the DMA system sometimes miscalculated the call capacity of the MCU as zero.
DMA-12212	6.0.2 P1	When an API-based participant mute command failed, the DMA system would log the failure in the call logs with the conference ID and participant ID values reversed.
DMA-12107	5.2.2, 6.0.2	On some DMA systems, large log archives were purged almost immediately as the system reached the log storage limit. The disk space available for log rotation has been increased from 1GB to 3GB.
DMA-12102	5.2.2, 6.0.2	If multiple ISDN gateways were available with equal metrics during the gateway selection process, the DMA system always distributed calls to the first ISDN gateway in the list instead of randomly distributing calls among the equivalent gateways.
DMA-12101	5.2.2, 6.0.2	During the ISDN gateway selection process, if one of the gateways had an unknown cost, the system stopped evaluating costs for any further ISDN gateways.
DMA-12100	5.2.2, 6.0.2	The DMA system did not exclude a busied out or out of service ISDN gateway MCU when selecting an ISDN gateway.
DMA-12071	6.0.2 P1	If a conference template was linked to an RMX conference profile that used the **Overlay** feature, calls using that conference template would fail.
DMA-12044	5.1, 5.2.2, 6.0.2	The DMA system sometimes leaked H.323 call objects when processing facility messages or performing call forwarding.
DMA-12029	5.1, 5.2.2, 6.0.2	If a primary cluster failed in a supercluster, the secondary cluster's database was sometimes not updated properly. This could result in network devices not registering properly to the secondary cluster.
DMA-11943	5.1, 6.0.2, 5.2.2	In rare circumstances, LDAP validation during the boot process could time out, preventing the DMA system from starting properly.

Issue ID	Found in Version	Description
DMA-11930	5.1.0	After you removed a cluster from a supercluster, the removed cluster was still shown in the DMA system's Dashboard and on the **Network > DMAs** page.
DMA-11920	6.0.2	A full backup and restore failed to restore custom certificates.
DMA-11797	5.1.0 P1, 5.2.2, 6.0.2	When an H.323 endpoint sent a registration request (RRQ) followed immediately by an unregistration request (URQ), and then sent another RRQ, the endpoint's registration was left in a bad state.
DMA-11788	6.0.2	Automatically created log archives couldn't be deleted after they had been downloaded. The DMA system failed to recognize that they had been downloaded.
DMA-11787	6.0.2	When conference rooms are created in the management interface, the DMA system does a case-insensitive check for conference ID uniqueness (for instance, Test and teSt are considered duplicates). But via the API, the DMA system failed to do a case-insensitive check, so it was possible to start two conferences using the conference IDs Test and teSt.
DMA-11716	5.2.2, 6.0.2	When using a "Resolve to external address" dial rule to resolve an H.323 URL, the DMA system performed SRV queries it shouldn't have. This resulted in calls to external endpoints failing.
DMA-11714	5.2.2.2, 6.0.2	Calls from a site that allows internet SIP calls via a session border controller (SBC) were not routed to the SBC.
DMA-11363	5.2, 6.0.2	If **Allow calls to/from rogue endpoints** was turned off on the **Call Server Settings** page, calls to endpoints registered to a different cluster in the supercluster failed.
DMA-9348	4.0.3 P4	On the **Admin > Conference Manager > Conference Settings** page, the **Default maximum bit rate** setting defaulted to 2048Kbps. The default value for this setting has been changed to **Unlimited**, and the configurable range now includes speeds up to 6144Kbps.

Issues Resolved in Version 6.0.2.1

The following table lists the issues resolved in version 6.0.2.1.

Issue ID	Found in Version	Description
DMA-11836	6.0.2	API: Attempting to create a conference template with telepresence layout mode set to ROOM_SWITCH returned an error.
DMA-11830	6.0.2	In the call flow for DMA-controlled VEQs, add a welcome message (General_welcome.wav) before the conference ID prompt (Conference_NID.wav).
DMA-11827	6.0.2	The default prompt set contained an unused prompt file, conference_join.wav.
DMA-11816	6.0.2	For calls to a conference room (VMR) via a virtual entry queue (VEQ), the call CDRs didn't contain the conference room pass-through value (userDataB).
DMA-11805	6.0.2	Auto-generated conference room IDs were limited to six digits, which was too few for some purposes. The length limit has been increased to 18.
DMA-11801	5.2.2.2	In a two-server cluster, the servers refresh their cached conference room data every 15 seconds. Whenever the data changed, a short-lived alert 3605 could occur because one server's cache was refreshed just before the change. The alert is now triggered only if the conference room counts differ for two refresh intervals in a row.

Issue ID	Found in Version	Description
DMA-11776	6.0.2 HF1	In order to be recognized as part of an Immersive Telepresence (ITP) room system, the endpoints (codecs) in the ITP system must follow this naming convention: <itp-room-name>_<number-of-displays>_<display-number> *Example:* Bainbridge_3_1 But if <itp-room-name> contained an underscore (*Example:* Bainbridge_OTX_3_1), the DMA system failed to recognize the devices as a single ITP system and didn't merge the ITP calls into a single CDR.
DMA-11767	6.0.2 HF1	The DMA system disallowed the '@' character in user IDs, preventing the use of email addresses as user IDs.
DMA-11734	5.2.2.2	When dialing out via RealPresence Access Director in order to add an external H.323 guest endpoint to a conference, the DMA system set the destination call signaling address to the IP address of the RealPresence Access Director system, causing the call to fail.
DMA-11682	6.0.2	An endpoint dialed a virtual entry queue (VEQ) hosted by one MCU and attempted to join a conference hosted by another MCU, which was out of video ports. The endpoint was disconnected without being played the "system is full" prompt.
DMA-11409	6.0.1	When a conference used a template linked to an RMX conference profile, the DMA system rejected API requests to start recording even though the conference profile enabled recording on request.
DMA-11405	5.1, 5.2, 6.0	API requests weren't being reported in the call and conference event records.
DMA-11077	5.2	If a call from the secondary endpoint (codec) in an Immersive Telepresence (ITP) room system arrived before the call from the primary codec, the DMA gatekeeper rejected it.
DMA-10036	5.0.2	When endpoints behind a VBP sent lightweight RRQ (keepalive) messages, the DMA gatekeeper misidentified them because the VBP uses the same endpointID for all of them (additive registration). The DMA gatekeeper now accepts their LRRQs without processing them.

What's New in the Version 6.0.2 Release

The Polycom DMA system version 6.0.2 includes the following new features (this is the first generally available version 6.0 release). For more information on these new features, see the *Polycom DMA 7000 System Operations Guide* and the online help.

❑ **Available in a package for virtual deployment**

In addition to the standard appliance edition, this version of the DMA system is available in an edition packaged for VM-based deployment in an organization's data center.

The version 6.0 software for the Virtual Edition of the DMA system is packaged as an Open Virtualization Archive (OVA) file. The OVA file contains the DMA application and information about its virtual machine environment. It can be installed as a virtual instance on a host machine running VMware® ESXi 5.0 or newer software. See "Server Hardware Profiles for a Virtual Environment" on page 14 for hardware requirements and performance information.

When deployed in a virtual environment, each DMA system instance runs in its own virtual machine and has the capabilities described in the previous section. The DMA instances can be superclustered (up to five), but not configured as two-server JBOSS clusters.

❑ **DHCP support**

To facilitate VM deployment, this version of the DMA system supports DHCP. When a new DMA system instance is started, it obtains an IP address from the DHCP server. Once the IP address is assigned, it is visible from the vSphere HA interface. The system administrator can then connect to the system using that IP address in order to configure the system, including assigning it static IP addresses.

❑ **DMA-controlled IVR services for VEQs**

This version of the Polycom DMA system supports a new type of virtual entry queue (VEQ) on supporting Polycom RealPresence Collaboration Server and RMX® MCUs (v8.1 or newer). The DMA system controls the new VEQs via API commands to the MCU hosting the VEQ call.

The prompts, slides, and call flow providing the IVR experience for a DMA-controlled VEQ reside on the DMA system. The DMA system validates the VMR number entered by the caller. If necessary, it re-prompts the caller a configurable number of times. If the caller fails to enter a valid number or requests an operator, the DMA system routes the call to the configured SIP URI for operator assistance (see operator assistance feature described below).

Like MCU-controlled VEQs, the DMA-controlled VEQs are a SIP-only feature and can be set up on the **Shared Number Dialing** page. See the online help for that page and for the **Add Virtual Entry Queue** or **Edit Virtual Entry Queue** dialog box for more information about VEQs and their configuration settings.

❑ **Support for custom prompt sets in DMA-controlled VEQs**

You can install multiple prompt sets in this version of the DMA system and assign one to each DMA-controlled VEQ. Each prompt set contains a set of audio prompts and video slides. You can customize the IVR experience (in terms of language or branding) associated with the call flow by installing custom prompt sets and creating DMA-controlled VEQs that use those prompt sets.

A prompt set is an archive (.zip) file containing a manifest file describing the prompt set and a collection of .wav and .jpg files with the individual audio prompts and video slides. You can add and manage prompt sets on the **IVR Prompt Sets** page. See the online help for that page for more information.

❑ **Support for operator assistance in DMA-controlled VEQs**

In DMA-controlled VEQs, operator assistance settings specify the SIP URI to which a call should be routed for operator assistance (help desk) and the configuration options governing when a call is routed to that URI. A call in the VEQ's IVR call flow is redirected to the specified operator or help desk URI when:

▫ No IVR resources are available.

▫ The caller failed to enter the correct conference ID or passcode a configurable number of times.

▫ The caller failed to respond to a prompt for a configurable number of seconds.

▫ The caller entered a configurable DTMF command to request operator assistance.

Each DMA-controlled VEQ has its own operator assistance settings for:

▫ The SIP URI to which to route the call for operator (help desk) assistance.

▫ The DTMF command for requesting an operator.

▫ The length of time after requesting an operator that a caller is given to cancel that request.

See the online help for the **Add Virtual Entry Queue** or **Edit Virtual Entry Queue** dialog box for more information about these and other VEQ settings.

❑ **Call/Conference History and CDR enhancements**

Call History detail records and CDRs have been expanded to include:

▫ For rejected SIP calls, the SIP code and reason.

▫ For SIP calls, model and version information for the originating and destination devices.

▫ For SIP ITP and TIP calls, the number of screens the room has.

▫ The minimum and maximum resolution used on the video channel and the content channel (available only for AVC calls using SIP signaling and a compatible Polycom RealPresence Collaboration Server or RMX MCU).

▫ Packet statistics (jitter, latency, and packet loss) for the video channel and content channel (available only for AVC calls using SIP signaling and a compatible Polycom RealPresence Collaboration Server or RMX MCU).

▫ For SIP calls, the INVITE's From header.

▫ The call ID of the originating and destination endpoint.

Conference History detail records and CDRs have been expanded to include the maximum number of resources (ports) used for the conference (available only for conferences on a Polycom MCU that provides this information).

See the online help for the **Call History** and **Conference History** pages, the **Call Details** dialog box, and the associated help topic **System Reports > Call Detail Records (CDRs)** for more information about call and conference history and the call and conference CDR layouts.

❑ **Resource priority support**

In an Assured Services SIP (AS-SIP) environment, a Local Session Controller (LSC) can provide priority-based precedence and preemption services to ensure that the most important calls get through. This version of the Polycom DMA system supports such resource prioritization mechanisms. A resource priority namespace and value can be assigned to each conference room. See the online help for the **Add Conference Room** dialog box for more information.

Conference rooms with no assigned resource priority use the system default specified on the **Conference Settings** page. See the online help for that page for more information.

The string `namespace:value` is used in the SIP Resource-Priority header of outbound calls from conference rooms (VMRs). For inbound calls that don't specify a resource priority, the DMA system provides the value assigned to the conference room to the MCU on behalf of the endpoint.

❑ **Improved Call Server Settings page**

The **Call Server Settings** page has been reorganized for greater clarity and usability. Three collapsible sections separate the general, SIP, and H.323 settings.

❑ **Configurable gatekeeper blacklist settings**

The system can be set to add H.323 endpoints to its blacklist (ignoring their signaling messages) when they send duplicate RRQ or GRQ messages in excess of configurable criteria. You can enable and configure this option on the **Call Server Settings** page. For each message type, you can specify:

▫ The threshold (number of duplicate messages) for blacklisting.

▫ The interval to which the threshold is applied.

▫ Whether blacklisted endpoints are also quarantined.

        ▫   Whether video border proxies can be blacklisted.

See the online help for the **Call Server Settings** page for more information.

❑ **ANAT support**

The system can be set to support Alternative Network Address Types (ANAT) signaling (RFC 4091 and RFC 4092) in the Session Description Protocol (SDP) for the purpose of negotiating IP version in a dual-stack (IPv4 + IPv6) environment. You can enable this option on the **Signaling Settings** page. See the specified RFCs for more information about ANAT signaling.

❑ **Configurable management connection whitelist**

The system can be set to accept connections to the management interface and API (port 8443) and to SNMP (by default, port 161) only from specified IP addresses or address ranges. This whitelist is enabled and configured on a new page, **Admin > Login Policy Settings > Access Policy Settings**. See the online help for that page for more information.

❑ **Greatly simplified History Retention Settings page**

Changes to the management of database table sizes and record purging have led to the removal of all configuration settings specifying the number of records of various types to be retained. The retention levels are now fixed at the values specified in "System Capabilities and Constraints" on page 3.

The only configuration options remaining are:

        ▫   Whether to retain Call Server registration history records.

        ▫   If retaining registration history, whether to include keep-alive messages.

        ▫   How many repeated low-value signaling messages (such as INFO messages about in-call status) to retain for a given call.

See the online help for the **History Retention Settings** page for more information.

❑ **Enhanced shutdown and restart functionality**

On the **Shutdown and Restart** page, it's now possible to shut down or restart a single server in a two-server cluster. See the online help for that page for more information.

❑ **Terminate conference after chairperson drops**

If this new conference template option is selected and the template is used for a conference with a chairperson passcode, the conference is terminated when the chairperson leaves the conference. A message is played to the remaining participants informing them that the chairperson has left the conference.

❑ **Delimiter change for DMA-controlled VEQ "speed dial" formats**

For DMA-controlled VEQ numbers, the DMA system recognizes two "speed dial" SIP dial string formats that enable callers to bypass the conference (VMR) number prompt or both it and the passcode prompt. The delimiter for these dial strings has been changed from a single star (*) to two stars (**), so the formats are now:

        ▫   `<veq number>**<vmr number>` — The system validates the VMR number. If it's valid, the caller bypasses the prompt for the destination conference. If the VMR has a conference passcode (PIN), chairperson passcode, or both, the system prompts for and validates the passcode.

□ `<veq number>**<vmr number>**<passcode>` — The system validates the VMR number, and if it's valid, the passcode. If both are valid, the caller bypasses both prompts and is placed directly into conference.

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

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

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

Software Version History

Only versions released for General Availability are listed.

Version	API Version	Release Date	Features
6.0.3	1.7.4	December 2013	Maintenance release to fix specific issues, plus conference template enhancements surrounding high resolution content.
5.2.2.5	1.2.2	December 2013	Maintenance release to fix specific issues.
5.2.2.4	1.2.2	October 2013	Maintenance release to fix specific issues.
6.0.2.1	1.7.2	August 2013	Maintenance release to fix specific issues.
5.2.2.3	1.2.2	August 2013	Maintenance release to fix specific issues.
6.0.2	1.7.1	July 2013	DMA-controlled VEQs with operator support, enhanced call/conference history and CDRs, resource priority (AS-SIP) support, ANAT support, gatekeeper blacklist, managaement connection whitelist, simplified history retention settings, single-server shutdown, new conference template setting.
5.2.2.2	1.2.2	July 2013	Maintenance release to fix specific issues.
5.2.1	1.2.1	March 2013	Maintenance release to fix specific issues.
5.2.0	1.2.1	December 2012	Cascading for size, mixed AVC/SVC conferences, FW NAT keep-alive, improved subscription events reporting, new MCU support, enhanced API control of MCUs, removal of XMPP server. Database changed from MySQL to PostgreSQL 9.2.1.
5.0.2	1.0.1	December 2012	Maintenance release to fix specific issues.
5.1.0_P1	1.1.0	December 2012	Maintenance release to fix specific issues.
5.1.0	1.1.0	November 2012	SVC conferencing, RFC 4575 support, untrusted traffic identification and handling, network setting changes, upgrade process monitoring, configuration-only backups.
5.0.1	1.0.1	September 2012	Maintenance release to fix specific issues.
4.0.3_P4		August 2012	Maintenance release to fix specific issues.

Version	API Version	Release Date	Features
5.0.0	1.0.0	July 2012	RealPresence Platform API, SNMP support, device authentication enhancements, SIP enhancements, log forwarding, ITP support enhancements, performance improvements.
4.0.3_P3		July 2012	Maintenance release to fix specific issues.
4.0.3_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 RealPresence Collaboration Server and RMX MCUs don't include their management IP address in the SAN field of the CSR (Certificate Signing Request), so their certificates identify them only by the CN. Therefore, in the Polycom DMA system, a Polycom MCU's management interface must be identified by the name specified in the CN field (usually the FQDN), not by the IP address.

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

❑ Superclustering is not supported.

❑ The Polycom DMA system can't be integrated with Microsoft Exchange Server and doesn't support virtual meeting rooms (VMRs) created by the Polycom Conferencing Add-in for Microsoft Outlook.

❑ Integration with a Polycom RealPresence Resource Manager or CMA system is not supported.

❑ On the **Banner** page, **Enable login banner** is selected and can't be disabled.

❑ On the **Login Sessions** page, the **Terminate Session** action is not available.

❑ On the **Troubleshooting Utilities** menu, **Top** is removed.

❑ In the **Add User** and **Edit User** dialog boxes, conference and chairperson passcodes are obscured.

❑ After **Maximum security** is enabled, management interface users must change their passwords.

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

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

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

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

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

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

▫ Minimum length is 15-30 characters (default is 15).

▫ Must contain 1 or 2 (default is 2) of each character type: uppercase alpha, lowercase alpha, numeric, and non-alphanumeric (special).

▫ Maximum number of consecutive repeated characters is 1-4 (default is 2).

▫ Number of previous passwords that a user may not re-use is 8-16 (default is 10).

▫ Minimum number of characters that must be changed from the previous password is 1-4 (default is 4).

▫ Password may not contain the user name or its reverse.

▫ Maximum password age is 30-180 days (default is 60).

▫ Minimum password age is 1-30 days (default is 1).

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

Session configuration limits:

▫ Sessions per system is 4-80 (default is 40).

▫ Sessions per user is 1-10 (default is 5).

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

Local account configuration limits:

▫ Local user account is locked after 2-10 failed logins (default is 3) due to invalid password within 1-24 hours (default is 1).

- Locked account remains locked either until unlocked by an administrator (the default) or for a duration of 1-480 minutes.

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

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

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

Server Hardware Profiles for a Virtual Environment

The following table describes the minimum and recommended server hardware profiles for each virtual machine (VM) with an instance of the DMA system. It also shows the typical performance capacities.

Component	Minimum Profile (Lab System)	Recommended Profile (Production System)
CPU	1-physical-core Westmere, 2.4 GHz or more CPU clock	8-physical-core Westmere, 2.4 GHz or greater CPU clock (e.g., 8x Intel Xeon E5620 @ 2.4GHz)
Memory	2 GB	8 GB
Disk	32 GB	146 GB
Performance	5 concurrent calls, 15 registrations	1200 calls, 12000 registrations

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

System Requirements

❑ For best reliability, deploy the Polycom DMA 7000 system into a good-quality IP network with low latency and very little packet loss.

- In systems with Active Directory integration, the network between the DMA system and Active Directory should have less than 200 ms round-trip latency and less than 4% round-trip packet loss.

- The network between clusters of a Polycom DMA supercluster should have less than 200 ms round-trip latency and less than 2% round-trip packet loss.

- The network between the Polycom DMA system and all MCUs should have less than 200 ms round-trip latency and less than 2% round-trip packet loss. Since this network carries only signaling traffic (the RTP stream goes directly from the endpoint to the MCU), bandwidth is not an issue.

- The network between the Polycom DMA system and video endpoints should have less than 200 ms round-trip latency and less than 6% round-trip packet loss.

❑ Computers used to access the management interface should have 1280x1024 minimum display resolution (wide screen, 1680x1050 or greater, recommended).

❑ Browser minimum requirements: Microsoft Internet Explorer® 7.0, Mozilla Firefox® 3.0, or Google Chrome 11 (with Adobe Flash plugin, not built-in Flash support).

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

Installation and Upgrade Notes

New System Installation

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

Existing System Upgrade

📧 *A version 6.0.x Virtual Edition DMA system can be upgraded to version 6.0.2.1 from the Maintenance > Software Upgrade page of the system's management interface. Deploying a new OVA file is not necessary.*

Follow the instructions in the online help for the Software Upgrade page to upload and install the upgrade package (.bin file). A new license is not required.

Polycom recommends taking a snapshot of your current instance of the DMA 7000 system before upgrading. See your VMware documentation for instructions.

Due to the change to the CentOS v6.4 operating system, it's not possible to directly upgrade to DMA version 6.0.2 from version 5.x or earlier versions. A fresh installation from disk is required. To prevent data loss, version 6.0.2 supports migrating backed-up configuration data from a version 5.x (Appliance Edition) system to version 6.0.2 (Appliance Edition or Virtual Edition).

📧 *Transaction (audit/history) data can be restored only from a full version 5.2.2.2 backup. For backups from any other 5.x version, only configuration data can be restored.*

See "DNS Records Requirement Changes" and, if applicable, "Version 5.0 to 5.1 IP Addressing Change" on page 16 regarding configuration changes you may need to make, depending on the version you're upgrading from.

The procedure for migrating to version 6.0.2 consists of these steps:

1. If the DMA system is running version 4.x, upgrade it to version 5.0.

2. Create a configuration-only backup or, if the system is running version 5.2.2.2 and you want to preserve transaction data, a full backup and download it to your PC.

3. For a migration to 6.0.2 Appliance Edition:

    a. Obtain the version 6.0.2 migration package and burn the ISO to disk.

    For instructions on how to obtain this package, see the support page for the DMA system:
    http://support.polycom.com/PolycomService/support/us/support/network/management_scheduling/dma_7000.html

    b. Perform a fresh install of 6.0.2 from disk as described in the *Getting Started Guide*.

4. For a migration to 6.0.2 Virtual Edition, obtain the OVA and deploy it as described in the *Getting Started Guide for a Virtual Environment*.

5. Upload the backup file you created prior to installing version 6.0.2.

6. Restore from the backup file. In the Confirm Restore dialog, you can elect to restore:
   - IP network configuration
   - Feature and system configuration
   - History, network usage, and log data (if you're restoring from a version 5.2.2.2 full backup)

📧 *Restoring feature and system configuration, but not network configuration (or vice versa) will result in invalid primary or backup cluster assignments for some territories. After the restore operation is complete, go to **Network > Site Topology > Territories** and assign primary and backup clusters to the affected territories.*

This upgrade requires a new license key after the upgrade.

Version 5.0 to 5.1 IP Addressing Change

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

When a single-server version 5.0 DMA system (unless configured for IPv6 only) is upgraded to version 5.1 or later, the previous version's virtual host name(s) and IP address(es) become the upgraded version's physical host name(s) and IP address(es). This is done because in prior versions, all access to the DMA system was supposed to use the virtual host name or IP address. Using the previous version's virtual host name(s) and IP address(es) as the new physical host name(s) and IP address(es) ensures that external devices can access the system without having to be reprovisioned.

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

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

DNS Records Requirement Changes

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

❑ A/AAAA records for both the physical and virtual host names are mandatory.

❑ The Embedded DNS feature requires a DNS NS record for the physical host name of each server in each cluster in the supercluster.

❑ NS records for the virtual host names must not exist.

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

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

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

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 this option.

Products Tested with This Release

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

Polycom recommends that you upgrade all of your Polycom systems with the latest software versions before contacting Polycom support. Any compatibility issues may already have been addressed by software updates. Go to http://support.polycom.com/PolycomService/support/us/support/service_policies.html to see the Current Interoperability Matrix.

Management Systems and Recorders	Version Tested
Polycom CMA	6.2.0.ER22
Polycom RSS4000	8.5
Polycom RealPresence Resource Manager	7.3.0,7.1.1
Gatekeepers, Gateways, SIP Servers and MCU's	**Version Tested**
Cisco 3241 Gateway	2.1(1.43)p
Cisco 3745	12.4

Cisco VCS	X7.2.2
Cisco Unified Communications Manager (CUCM)	9.0.1
Cisco Telepresence Server (TPS)	2.3
Cisco CTMS	1.9.2
Cisco ASR-1002F	3.7.2
Codian 4505 MCU	4.2,4.4(3.49)
Lync 2010 Edge Server	4.0.7577.205 CU7
Lync 2010 Media Server	4.0.7577.205 CU7
**Lync 2013 Edge Server	5.0.8308.291 (CU1)
**Lync 2013 Media Server	5.0.8308.291 (CU1)
Polycom CMA	6.2.0.ER22
Polycom MGC	9.0.4.3
Polycom MGC Gateway	9.0.4.3
Polycom RMX 1500, 2000, 4000	8.1
Polycom Real Presence Collaboration Server 800s	8.1
Polycom RMX Gateway	8.1.6
Polycom RMX1000	2.1.2
Radvision ECS Gatekeeper	7.1.2.12
Radvision Scopia P10 Gateway	5.7.2.0.25
Tandberg Gatekeeper	N6.1
Tandberg Gateway	G3.2
Endpoints	**Version Tested**
Aethra X7	12.1.7
Cisco C20	6.0.1, 6.1.1
Cisco C40	5.1
Cisco C60	5.1
Cisco C90	6.0.1, 6.1.1, 5.1.3
Cisco E20	4.1.1,4.1.2
Cisco EX90	5.1.3,6.0.1, 6.1.1
Cisco SX20	6.0.1, 6.1.1
Cisco CTS	1.9.1
Cisco TX	1.9.1
IBM Sametime Connect Client	8.5.2 IFR1
LifeSize Desktop client	2.0.2.191
LifeSize Express 220	4.11.13
LifeSize Passport	4.11.13
LifeSize Room	4.7.21,4.7.22
LifeSize Team 200	4.7.21,4.7.22

LifeSize Team 220	4.11.13
Microsoft Lync 2010	4.0.7577.4384
Microsoft Lync 2013	15.0.4481.1000
Polycom CMAD	5.2.3,5.2.4
Polycom DST Broad 5	2
Polycom DST K60	2.0.1
Polycom FX	6.0.5
Polycom Group Series Touch Controller	4,4.1.1
Polycom HDX	3.1,3.1.1.3, 3.1.2
Polycom PVX	8.0.16
Polycom OTX/TPX	3.1.1-1
Polycom RPX	3.1.1-1
Polycom QDX4000	4.0.2
Polycom QDX6000	4.0.3
Polycom RealPresence Desktop	2.0,3
Polycom RealPresence Group Series	4.0,4.1.1
Polycom RealPresence Mobile Android	2,3
Polycom RealPresence Mobile iPad	2,3
Polycom SoundPoint 601 SIP	3.1.7
Polycom SoundPoint 650 SIP	4.0.3
Polycom SoundStation IP4000 SIP	3.1.7
Polycom SoundStation IP7000	4.0.3
Polycom Telepresence M100	1.0,1.0.5
Polycom HDX Touch Controller	1.6,1.7
Polycom VSX	9.0.6.2
Polycom VVX1500	4.0.2,4.0.4
Polycom VVX500	4.1.3
Polycom VVX600	4.1.3
Radvision Scopia XT1000	2.5.308,2.5.416
Radvision Scopia XT5000	3.0.122,3.1.1.37
Siemens OpenScape Desktop Client WE	V7 R0.0.6 (70.0.0.0006)
Siemens OpenScape Media Server	V7.00.01.ALL.07_PS0010.E11
Siemens OpenScape UC	V7.00.01.ALL.07_PS0010.E11
Siemens OpenScape Voice	V7.00.01.ALL.07_PS0010.E11
Siemens OpenStage Phone	V3_R1_31_0
Sony PCS-1	3.42
Sony PCS-G50	2.72
Sony PCS-TL50	2.42

Sony PCS-XG80	2.34,2.36
Tandberg 150 MXP	L6.1
Tandberg 1700 MXP	F9.3.1
Tandberg 6000 MXP	F9.3.1
Tandberg Edge95 MXP	F9.1.2,F9.3.1
**Lync 2013 is tested and supported for "meet on the bridge" (VMR) dialing. No other call scenarios are tested or supported.	

Resolved Issues

The following table lists the issues resolved in the Polycom DMA 7000 system version 6.0.2 base release. See "Issues Resolved in Version 6.0.3" on page 6 for issues resolved in the subsequent maintenance releases.

Issue ID	Found in Version	Description
DMA-11567	5.1, 5.2, 6.0	A race condition between the thread joining a call to conference and the thread reading the conference and participant information from the MCU sometimes led to termination of the call.
DMA-11559	5.2, 6.0	Transfer of site link throttlepoint data across clusters failed.
DMA-11543	5.1, 5.2.2 P1	The DMA system failed to prefer SVC-capable MCUs when routing calls to a Mixed AVC and SVC mode conference.
DMA-11337	5.0.2 P1 HF1	When an API client that's subscribed to conference notifications failed to respond to a notification, the DMA system waited indefinitely. Subsequent notifications to that client were queued up without limit, consuming large amounts of memory. Now, the system discards a notification if it receives no response within 10 seconds, and it sends the next notification in the client's queue. The notification queue for a client is now limited to 500. If it reaches that limit, the system discards the oldest notification in the queue. Also fixed in 5.2.2.
DMA-11323	6.0.2	In CDRs for calls that came through a session border controller (SBC), the origModel field was always "HDX8000" regardless of the actual endpoint model.
DMA-11285	5.2	The DMA system intermittently lost connection to a Cisco MSE 8000 MCU.
DMA-11265	5.2.1	Deadlocked SIP threads sometimes caused SIP calls and registrations to fail.
DMA-11150	5.2	The system took 60 seconds or more to respond to LWRRQs (light-weight registration requests). Also fixed in 5.2.2.
DMA-11146	6.0.0	The system experienced long pauses (up to 30 seconds) due to virtual memory thrashing and 100% disk usage. Also fixed in 5.2.2.
DMA-10894	5.0	Database audit purge continued to purge after it should have stopped. Also fixed in 5.2.2.
DMA-10884	6.0.1	Anonymous users could access the LDAP database via port 4449 and access configuration and user data for the system. Also fixed in 5.2.2.
DMA-10729, 10348	5.2	A two-server cluster sometimes experienced data synchronization issues in reboot or failover situations. Also fixed in 5.2.2.

Issue ID	Found in Version	Description
DMA-10636, 9312	5.0	If either (a) the active server in a two-server cluster failed over to the backup server or (b) the primary cluster for a territory failed over to the backup cluster, a conference for which the failed server or cluster was responsible could continue without the backup server or cluster taking over signaling for it. If a new (or dropped) participant dialed into the same conference room (VMR), the backup server or cluster started a new conference. This resulted in two active conferences for the same VMR. 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. Also fixed in 5.2.2.
DMA-10561	5.2	The system leaked memory when an API client used certain conference commands. Also fixed in 5.2.1 and 5.0.2.1.
DMA-10430	5.2, 6.0	Point-to-point SIP calls failed for endpoints that register a contact URI without port, such as the LifeSize Team 220. Also fixed in 5.2.1.
DMA-10314	5.2, 6.0	If a non-numeric conference room was used, SVC endpoints weren't notified of all the media streams and effectively received a video switching (VSW) experience. Also fixed in 5.2.1.
DMA-10208	5.2	In a two-server cluster running on Dell R620 servers, the private network connection between the two servers randomly failed. Also fixed in 5.2.2.
DMA-10143	5.2	When a two-server cluster was placed into maximum security mode, one of the servers remained in the previous security mode.
DMA-10111	5.2	RMX MCUs have a per-conference limit of 160 (MPM+ cards) or 180 (MPMx cards) participants. A conference with large numbers of CIF participants could reach this limit and still have capacity available. The DMA system would see capacity still available on the current MCU, so rather than create a cascade link to another MCU, it continued to send calls to current one. These calls were rejected.
DMA-9873	5.1	Under rare circumstances, the DMA system processed an incomplete SIP message received over TCP and forwarded it to a downstream device. DMA hid the fact that the message was incomplete (its content was shorter than indicated in the Content-length header) by changing the Content-Length header to reflect the shortened content. This happened when the DMA system received an incomplete SIP message and the remaining part didn't arrive within 2 seconds. It then terminated the TCP connection, but processed the incomplete message.
DMA-9855	5.0.1, 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 was included in version 5.0.2.
DMA-9740	5.0, 5.2, 6.0	Dial-outs to an address that resolved to a SIP peer failed.
DMA-9687	5.0, 5.1	SIP signaling threads sometimes deadlocked.

Issue ID	Found in Version	Description
DMA-9080	4.0.3 P1 HF1	**Network Settings**: For 1000Base-T, when **Auto-negotiation** was turned off and **Speed** set manually, after rebooting, **Auto-negotiation** was back on. This is working as designed; according to the IEEE specification, auto-negotiation is mandatory for 1000Base-T. DMA-9241 in the Known Issues list is tracking the issue that the system shouldn't allow **Auto-negotiation** to be turned off in the first place.
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-6290	4.0	Due to call signaling timing issues, endpoints joined to a conference sometimes failed to receive audio.

Known Issues

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

Issue ID	Found in Version	Description	Workaround
DMA-11966	6.0.2.1	Password complexity requirements are too stringent for the Polycom DMA system, Virtual Edition restricted console.	The first time you log in to the restricted console, you will be required to change the password for the *polycom* account. Use a password with the following characteristics: • At least 6 characters in length • Not a dictionary word • Not a palindrome (spelled the same forward and backward) • Not simply a case change of the previous password • Not a letter rotation of the previous password (*polycom* -> *mpolyco*)
DMA-11919	6.0.2 P1	A user whose username contains a backslash character is unable to log in to the system.	

Issue ID	Found in Version	Description	Workaround
DMA-11840	5.2.2 P3	In some rare circumstances, when the DMA system responds to a Session Description Protocol (SDP) Offer message, the SDP Answer response does not include all "m=" lines. This behavior can lead to call release.	
DMA-11556	6.0.2	For calls from Interactive Telepresence (ITP) rooms using SIP (not TIP) signaling, many fields in the call CDR contain an escaped (quote-enclosed) comma-separated list of values (one for each screen in the ITP system) instead of a single value. When the call CDR .csv file is opened using Microsoft Excel, it may misinterpret the escaped comma-separated list as a single large integer. The online help and Operations Guide don't include the above information.	
DMA-11493	6.0.2	On the **Reports > Call History** page, limiting a search to a specific territory doesn't work.	Specify a cluster or site.
DMA-11479	6.0.2	While viewing associated conferences for a conference in the **Reports > Conference History** list, if you repeatedly select other entries before the current query has finished, the DMA system can report a database access error and the web interface can become unresponsive.	Allow time for each associated conference query to complete before selecting another conference.
DMA-11442	6.0	API: Conference updates may contain null endpoint-identifier values.	
DMA-11432	6.0.2	Setting the Gathering Settings Info fields to more than 80 characters via the API results in a 500 – Internal Server Error.	Limit the text in these fields to 80 characters.
DMA-11425	6.0.2	On the **Active Calls** page, the destination of a VMR call is sometimes shown as the originating endpoint.	
DMA-11409	5.x, 6.0	If a conference is using a RealPresence Collaboration Server or RMX profile that has recording enabled, the DMA system is unaware of that and rejects attempts to start recording via the API.	Use a "standalone" conference template (a free-standing template defined in the DMA system) that has recording enabled, not a template linked to a conference profile on the MCU.
DMA-11402	5.0.2 P2, 6.0.1	API: After a cluster in the supercluster was disconnected and reconnected, conference participant information from that cluster was out of sync with participant information from other clusters.	
DMA-11319	5.2.1	The DMA system doesn't support H.245 encapsulation or FastConnect. But when an endpoint sends a startH245 Facility message, the system passes that message on to the MCU hosting the conference. It should either ignore the message (not pass it on) or use the h245Address in the message if it's different from the h245Address supplied in the connect message.	

Issue ID	Found in Version	Description	Workaround
DMA-11290	6.0.2	On the **Site Statistics** page, a new call in any site appears in all sites.	
DMA-11225	6.0.1	When a call to a VEQ is transferred to a VMR on another MCU, the call history shows the destination as the IP address for the first (VEQ) MCU.	
DMA-11175		The **Conference Manager Usage** pane on the dashboard failed to show the correct number of audio-only calls when they exceeded the maximum number of voice ports.	
DMA-11168	5.0.2 P1 HF1	When the DMA system is in direct mode, calls from an endpoint behind a VBP or on a neighbored system to another endpoint behind a VBP or on a neighbored system, or to a VMR on a neighbored system, can remain in the Active Calls list indefinitely.	Do one of the following: • Enable routed mode. • Use an ALG/SBC that allows or responds to IRQ messages, and on the **Call Server Settings** page, enable **Terminate calls based on failed responses to IRQs**.
DMA-11135	6.0.2	The **Add/Edit Direct Dial Virtual Entry Queue** dialog boxes don't include the **DMA-based IVR Call Flow** settings, so if an "External IVR control" entry queue is selected, the call flow can't be properly configured (prompt set, timeouts, etc.).	
DMA-11049	6.0.1	If an RMX MCU is added to the DMA system as a conferencing resource first, and then attempts to register with the DMA gatekeeper, the registration fails.	Register the MCU with the DMA gatekeeper before adding it as a conferencing resource.
DMA-10896	5.0.2 P2, 6.0.1	The DMA system can't be configured for IPv6 only via the USB Configuration Utility.	Use the alternate procedure (configuring without a USB stick) in the Getting Started Guide.
DMA-10860	6.0.1	User with only Provisioner role can't access **Reports > Orphaned Groups and Users**.	Log in as a user with Administrator role to access that page.
DMA-10856	6.0	For AD users, the CMA system's user-to-device associations aren't available in the DMA system.	
DMA-10812	6.0	After the DMA cluster responsible for AD integration failed to update its cache due to a change in AD credentials, it failed to display alerts 2101 and 2107.	
DMA-10777	6.0	In gateway calls (SIP – H.323) between the following endpoints, one side failed to get video: • LifeSize Room 200 and Cisco (Tandberg) 6000 MXP • LifeSize Room 200 and Polycom RealPresence Desktop • Cisco (Tandberg) 6000 MXP and Polycom RealPresence Desktop	
DMA-10771	6.0	If the DMA system is configured to validate certificates for server connections, it can't be integrated with RealPresence Resource Manager or CMA versions prior to 7.3.	Upgrade the RealPresence Resource Manager or CMA system to 7.3.

Issue ID	Found in Version	Description	Workaround
DMA-10734	6.0	The **Network Settings** page continued to indicate a configuration mismatch between servers in a two-server cluster after the mismatch was corrected.	
DMA-10372	6.0	After an MCU became unavailable, SIP calls were successfully moved to another MCU, but content sharing was not.	
DMA-10300	5.1.0 P1 Hotfix 2, 6.0	In a cascaded conference, when the hub MCU became unavailable and the endpoints on it dialed back in, they correctly rejoined on a spoke MCU, but their user interfaces showed only a single endpoint in conference.	
DMA-10247	5.0.0 Hotfix 2	The DMA system manages bandwidth incorrectly for SIP endpoints registered through a RealPresence Access Director system that is using software version 3.0 or below.	Upgrade the RealPresence Access Director system to software version 3.1 or later.
DMA-10125	5.2	Cascade links stay up for a long time after there are no more participants on the cascaded MCU.	
DMA-10013	5.2	IPv6 VEQ calls failed to reach the VMR.	
DMA-9992	4.0.2	When a Cisco (Tandberg) EX90 endpoint using H.323 is in a call with an HDX endpoint using SIP, minor video artifacts may be seen on the Cisco endpoint.	
DMA-9991	4.0.1	When a Cisco (Tandberg) MXP 6000 endpoint using H.323 calls an HDX endpoint using SIP, the Tandberg endpoint doesn't receive video.	
DMA-9971	5.0.1	The DMA MIB couldn't be loaded into a Zenoss 3.2.1 network manager.	Download the MIB and in a text editor make the following changes in the IMPORTS section: • 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-9859	5.2	API: There is a redundant nesting of the mcu-pool-identifier xml tag.	
DMA-9854	5.1	When a Cisco SX20 endpoint dialed into a VMR, it connected but didn't receive video.	The Cisco SX20 endpoint is not currently supported.

Issue ID	Found in Version	Description	Workaround

DMA-9775	5.1	Call didn't connect dialing from Acme HDX h.323 to RPAD side VMR through h.323 trunk using 'id@ip' as dial string.	Add following script as preliminary for 'Resolve to conference room ID' dial rule: (change *<ip>* to external ip of your enterprise edge server):
			
			if(DIAL_STRING.match(/[0-9]{4}@*<ip>*))
			{
			vmr = DIAL_STRING.replace(/([^@]*)@.*/i,"$1") ;
			println(vmr);
			DIAL_STRING=vmr;
			}

DMA-9735	5.1, MFW 0.3.0	Null pointer error when updating call properties for media streams.	
DMA-9708	5.0	The default Request URI format option for the postliminary of a SIP peer is equivalent to the template: #pscheme#:#oruser#@#phost# The #pscheme# placeholder is the peer's scheme. This becomes "sips" if the peer's transport type is configured as TLS, even if the original Request URI's scheme was "sip." Some SIP peers, such as the Cisco SBC, won't accept "sips" in the Request URI if other headers contain "sip." The same problem will occur if any other format option that uses #pscheme# is selected.	To prevent such failures, do the following: 1. In the **Edit External SIP Peer** dialog box for the peer, go to the **Postliminary** tab. 2. Under **Request URI options**, change **Format** to **Free Form Template**. 3. In the **Template** field, replace #pscheme# with #orscheme# so that the Request URI template looks like this: #orscheme#:#oruser#@#phost#
DMA-9700	5.1	H.323 calls to an Aethra X7 endpoint using the DMA system as gatekeeper disconnect within one minute.	On the DMA system's **Call Server Settings** page, turn off **Terminate calls based upon failed responses to IRQs**.
DMA-9670	5.1	SIP calls gatewayed by the DMA system to a RealPresence Access Director configured as an external H.323 gatekeeper fail because the gatekeeper doesn't have enough information to route the call. This happens because the LRQ that the DMA system sends to the gatekeeper contains only the E.164 digits, not the domain information, in destinationInfo.	On the DMA system's **Call Server Settings** page, turn on **For SIP calls gatewayed to an external gatekeeper, use the H.323 email ID as the destination instead of the E.164 number**. **Note:** This option affects communications with all external H.323 gatekeepers to which the DMA system gateways SIP calls.
DMA-9579	5.1	When calls to a VMR are rejected due to no capacity, in the conference history and CDR they aren't associated with the conference they tried to join.	To correctly associate such a call with the conference it attempted to join, match the call's destination string with the VMR number in the conference CDR.
DMA-9550	6.0, MFW 0.3.0	DMA system doesn't restrict endpoint bandwidth for SVC calls.	
DMA-9524	5.0.1	Territory ownership information displayed on the dashboard is sometimes incorrect.	
DMA-9506	5.1	When the USB Configuration Utility was used to configure a single-server system to use IPv6 only, the IPv6 network settings weren't properly implemented and the system didn't start.	

Issue ID	Found in Version	Description	Workaround
DMA-9496	5.1	When the USB Configuration Utility was used to configure a single-server system to use IPv4+6 and split networking, the IPv6 signaling network settings weren't properly implemented.	
DMA-9463	5.1	When an external endpoint's registration request is proxied to the DMA system by a RealPresence Access Director SBC, the DMA system incorrectly associates the endpoint with the "Internet/VPN" site instead of the site to which the RealPresence Access Director belongs.	
DMA-9361	5.0.1	In a superclustered environment, some call events may appear out of order on the **Call Events** tab of the **Call Details** dialog box.	
DMA-9325	5.0	On the **Call History** page, records found by a dial string search may have an empty **End Time** field even though they have an end time.	
DMA-9324	5.0	When a rogue or neighbored call traverses two or more DMA clusters within one second, the call records from the clusters aren't always merged correctly, leading to inconsistent Call History information. **Note:** This problem is resolved for callers managed by one of the clusters in the supercluster.	
DMA-9241	5.0	Auto-negotiation is mandatory for 1000Base-T, but the DMA system allows it to be turned off.	Don't attempt to turn off auto-negotiation if you have a 1000Base-T network.
DMA-9139		The DMA system doesn't support CMA or RealPresence Resource Manager address book services for H.320 devices.	
DMA-9131		When a call forwarding loop involves an endpoint with multiple lines, the call keeps ringing that endpoint and can't be ended by the calling endpoint.	
DMA-9128	5.0	The **Users** list can't be sorted on the **Associated Endpoints** column.	
DMA-9115	4.0.3 P1	The DMA system creates an active call entry for an OCS chat INVITE.	
DMA-9098	4.0.3	MCUs added to a DMA system prior to version 4.0 are deleted 30 days after upgrading to version 4.0 or later.	Working as designed. After upgrading, edit each MCU. In the **Edit MCU** dialog box, select **Permanent** to prevent the MCU's registration from expiring.
DMA-9085, 9088	5.0	On the **Resource Management Server** page, **Model** is "CMA" for a RealPresence Resource Manager system.	
DMA-9027	4.0.3	If SIP device authentication is enabled, it can be turned off for a specific endpoint, but not for a SIP peer.	
DMA-9010	5.0	Sony PCS-1 and PCS-G50 endpoints are unable to remain connected in H.323 calls when they're registered to the DMA gatekeeper.	

Issue ID	Found in Version	Description	Workaround
DMA-8975	5.0	Attempt to edit an MCU with active calls. The system displays an error message stating that it can't be deleted when there are active calls or conferences."	
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-8912	4.0.3 P1	Under certain circumstances the status between local DMA clusters is incorrect even though the servers continue to function properly.	
DMA-8906	4.0.3 P1	DMA UI allows host name and domain name entries of invalid length.	Limit host name and domain name to a combined maximum of 64 characters.
DMA-8904	5.0	On dial-outs from a VMR, the system incorrectly records the originator of the call as the endpoint called (affects **Active Calls**, **Call History**, and CDRs).	
DMA-8885	5.0	When a caller with a higher quality of service (QoS) setting dials into a conference and there isn't sufficient bandwidth, lower QoS calls are correctly dropped, but the higher QoS caller must redial in order to get into the conference.	
DMA-8875	5.0	When a conference uses a custom template with auto layout enabled, auto layout sometimes doesn't work.	
DMA-8869	5.0.1	When a VMR call that traverses two DMA clusters and is pinned to the **Active Calls** list ends, its **Destination** field reverts from the MCU name to the dialed digits.	
DMA-8836	5.0	Integrating the DMA system with a RealPresence Resource Manager doesn't automatically integrate the RealPresence Resource Manager with the DMA system (that is, connect it to the DMA system's API).	On the RealPresence Resource Manager, integrate it with the DMA system. The integration of the DMA system back to the RealPresence Resource Manager is automatically created.
DMA-8818	5.0	At certain display resolutions and/or browser window sizes, some DMA dialog boxes may be cut off.	Use at least the minimum supported display resolution (1280x1024) and maximize the browser window.
DMA-8815	5.0	When an RMX MCU is in dual stack (IPv4 + IPv6) mode, the DMA system attempts to respond to it via IPv6 even though it's in IPv4-only mode.	
DMA-8791	5.0	When an RMX MCU registers with Call Server, its internal 172 address may appear in the list of media IP addresses.	The DMA system receives this IP address from the RMX MCU and simply reports it.
DMA-8715	5.0	Removing a cluster from the supercluster may cause Adobe Flash to crash.	In a new browser window, log back in.

Issue ID	Found in Version	Description	Workaround
DMA-8675	5.0	On calls to VMR, DMA system shows different requested and final bit rates than the MCU and endpoints show.	
DMA-8601	5.0	Downloading call detail records (CDRs) can take a long time (> 2 minutes) when there are many CDRs in the system.	
DMA-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 Lync 2010 client to a DMA VMR hosted on an RMX 1500 MCU don't receive video.	Use an RMX 2000 or 4000 MCU.
DMA-7981	5.0	In the call CDRs of VMR calls, the userRole field for participants is often null.	
DMA-7834	4.0, 4.0.3	In rare instances, an upgrade or rollback can result in not being able to log in to the GUI as any user.	Reboot the DMA.
DMA-7829	4.0.3	Integration to Microsoft Active Directory server sometimes fails with the message "Cache loading failed" and an alert icon with hovertext "Loading of the cache failed. Error: Timed out waiting for data from the directory." 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-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.

Issue ID	Found in Version	Description	Workaround
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.	
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, 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.

Issue ID	Found in Version	Description	Workaround
DMA-6103	3.0	In an environment with both a DMA system and a Cisco Unified Conference Manager (CUCM), video path problems were encountered if certain endpoints (Cisco 9971, Polycom HDX9002, and Polycom V500) were registered to the CUCM.	Register the endpoints to the DMA system.
DMA-6101	4.0	Under some circumstances, it may become impossible to log into one server of a two-server cluster because of a heartbeat failure stemming from a time disparity between the two servers.	Use NTP to synchronize the time on both servers and reboot the servers.
DMA-6033	4.0	On the Conference Settings page, the DMA system's default maximum bit rate setting defaults to 2048, and that limit applies to both conference and non-conference (Call Server) calls. This may cause calls to or from Immersive Telepresence (ITP) systems requiring higher bit rates to fail.	On the Conference Settings page, change the default maximum bit rate setting to Unlimited.
DMA- 5862	3.0	HDX endpoints expect H.323 bandwidth to be reserved in 64 kbps increments, but the DMA system uses smaller increments. The DMA system may, for instance, allocate 498 kbps for a call, and the call will use that. But the endpoint displays 448 (64 * 7).	
DMA- 5337	3.0	The DMA system doesn't properly handle SIP signaling from Polycom V-series endpoints with firmware prior to v. 9.0.6 (Feb 02, 2010).	Upgrade the endpoints to v. 9.0.6 or later.
DMA-5313	3.0	The Property Changes tab of the Call Details dialog box sometimes contains entries with duplicate sequence numbers.	
DMA- 5069	3.0	In a superclustered environment, slight time drifts between clusters may produce CDR records out of order or duplicated. 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.

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- 3390	2.3	If a DMA cluster is the primary or backup for a territory, it could be removed from the supercluster via the USB Configuration Utility with no warning that territory responsibilities need to be corrected afterward.	After removing a cluster from a supercluster, always check and correct territory responsibilities.
DMA- 2797	2.3	Some Sony endpoints that register with the DMA system become unregistered after five minutes.	
DMA- 2717	2.2	If a "spoke" MCU with a cascade link to the "hub" MCU is registered with an unavailable GK, callers on the two MCUs are isolated from each other. No indication in GUI or logs.	Do one of the following: 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-2109	2.3	Polycom V500 endpoints don't support failover of SIP registrations.	
DMA- 2014	2.3	Polycom HDX and PVX endpoints don't support failover of SIP registrations.	
DMA- 1939, 1941, 1948	2.3	H.323 calls using dial strings of the form <IP Address>##<Alias> sometimes fail.	The DMA supports such dial strings for both inbound and outbound calls, routing them to the specified gatekeeper or MCU IP address. Interpretation of the alias depends on the destination gatekeeper or MCU. Use of this feature is not recommended, however, because support for it varies significantly among different kinds of endpoints.

Where to Get the Latest Product Information

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