Polycom® CMA® System

Polycom is pleased to announce this v6.2.5 release of the Polycom® Converged Management Application™ (CMA®) system.

Contents

Software Version History

Version	Release Date	Features
6.2.5	August 2013	The CMA system v6.2.1 through v6.2.5 releases are maintenance releases only. See Resolved Issues on page 12 for information about the issues resolved in these releases.
6.2.4	June 2013	
6.2.3	April 2013	
6.2.2	January 2013	
6.2.1	December 2012	
6.2.0	November 2012	See About the CMA System v6.2.0 Release on page 2.

Polycom CMA System Service and Support Notice

All Polycom CMA service contracts end on or before July 31st, 2015. However, Polycom code fixes to the software will end on July 31, 2014 with the following exceptions:

1 Escalations with a severity of P1, as defined in the applicable service description, may be considered for resolution with a code fix.

2 Security-related escalations regardless of severity may be considered for resolution with a code fix.

3 All other escalations are eligible for troubleshooting support by Polycom Global Services (PGS) for verification as a known issue.

Notes
- To be considered for a code-fix resolution, the CMA system must be running v6.2.5.
- After July 15th, 2014, Polycom will not provide new code fixes for the Polycom CMA system; however, PGS will continue to take escalations and provide troubleshooting support and known issue verification until July, 2015.
- Service contracts that expire on or before July 14th, 2014 are not eligible for software support after that date.

About the CMA System v6.2.0 Release

The v6.2.0 release of the CMA system included the following new features:

- Support for Polycom® RealPresence® Group Series Solution
- RealPresence Group Series Touch Control Software Updates
- Support for RealPresence Desktop Video Collaboration Software
- Enhanced Management of E.164 Numbering for Dynamically-Managed Endpoints

Support for Polycom® RealPresence® Group Series Solution

The CMA system v6.0 release provides support for the Polycom RealPresence Group Series. It provides standard support for the following functionality:

- Authentication
- Scheduling
- Monitoring
- Presence
- Call Detail Records (CDRs) and CDR reporting

It also provides specialized support for the following functionality (as described in the sections that follow):

- Provisioning
- Software UpdatesSoftware Updates
- Management

Note that RealPresence Group Series systems are managed in dynamic management mode only. For more information about dynamic management mode, see the P*olycom CMA System Operations Guide*.

> **IMPORTANT**
> If in your environment, RealPresence Group Series systems have already registered with the CMA system v6.0.x (or earlier) gatekeeper, delete them from the CMA system just before you upgrade to CMA system v6.2. Then once the CMA system has been upgraded, allow them to re-register. Otherwise, the Group Series systems may each consume two licenses and the data reported for them may be inconsistent.

Provisioning

In the v6.2.0 release, the CMA system extends its automatic and bundled provisioning capabilities to the new RealPresence Group Series systems.

Administrators can create and lock down automatic and bundled provisioning profiles in order to enforce company policies around network usage, endpoint support, user experience, and security.

The CMA system does not support scheduled provisioning functionality for RealPresence Group Series systems.

Software Updates

Because RealPresence Group Series systems are dynamically managed, the CMA system v6.2.0 release can perform automatic software updates on the systems. When a RealPresence Group Series system starts up (and at designated intervals thereafter), it can be configured to automatically poll the CMA system for a software update package. If a newer software update is available, the package is sent to the endpoint in XML format over a secure HTTPS connection.

The CMA system does not support scheduled software update functionality on RealPresence Group Series systems.

Management

The CMA system v6.2.0 offers standard management support for RealPresence Group Series systems. It performs the following management functions:

• View Details	• Reboot Device
• Search Devices	• Manage Owner
• Connect or Disconnect	• View Peripherals
• Manage	• Associate User
• Send Message	• Assign Area

Because RealPresence Group Series systems are dynamically managed, they cannot be manually added or edited in the CMA system. Instead, the endpoint systems must be configured with the required address and credentials to poll the CMA system, as the provisioning server, for configuration information.

RealPresence Group Series Touch Control Software Updates

The CMA system v6.2.0 can also perform automatic software updates of the RealPresence Group Series Touch Control software. Note that the software update packages for the RealPresence Group Series Touch Control device are distinct from the software update packages for the HDX Touch Control device.

Support for RealPresence Desktop Video Collaboration Software

In the v6.2.0 release, the CMA system's support for the new RealPresence Desktop video collaboration software includes standard:

- Directory Support
- Scheduling
- Reporting
- License Entitlement Management

With regard to license entitlement, each active RealPresence Desktop instance consumes a license. If a user logs into multiple RealPresence Desktop instances at the same time using the same credentials, each instance will consume a license. The CMA system can be configured to reclaim inactive RealPresence Desktop licenses. For more information, see the P*olycom CMA System Operations Guide*.

Enhanced Management of E.164 Numbering for Dynamically-Managed Endpoints

In the v6.2.0 release, the CMA system allows administrators to control and configure the E.164 number used to reach dynamically-managed endpoint systems.

To apply the E.164 numbering scheme to an endpoint system, it must be dynamically managed and have H.323 enabled, which can be done during automatic provisioning.

The CMA system will apply the E 164 numbering scheme to all dynamically-managed endpoints registering to the system only if no other E.164 alias has been previously provided in a dial string reservation.

When implementing an E.164 numbering scheme, go to **Admin > Dial Plan and Sites > E.164 Numbering Scheme**. The following options are available:

Field	Description
Prefix	• **No Prefix**—The system will not append a prefix to create the E.164 assignment. • **A Number**—The system appends the prefix specified to create the E.164 assignment. • **Based on Device Type**—The system appends a pre-defined Device Type suffix to create the E.164 assignment.
Base Field	• **Specify Number Range**—Identify a number range to be used. The system uses a number from this number range to create the E.164 assignment. • **Use Phone Number**—The system will use a portion of the user's phone number to create the E.164 assignment. The phone number information can be accessed from either the Active or local directory. • **Maximum number of digits to use** from the user's phone number (between 3 and 10 digits). • **Number range to use if phone number is empty** (reverts to **Specify Number Range**)—The system will revert to using a number range if the user's phone number is empty.
Suffix	• **No Suffix**—The system will not append a suffix to create the E.164 assignment. • **A Number**—The system appends the suffix specified to create the E.164 assignment.

Notes

• The total number of digits specified for an E.164 number must be 15 or less. If the user's phone number is assigned to the Base Field, the system reserves one digit to differentiate between the user's multiple devices. In this case, the total number of digits configured cannot exceed 14 digits.

• The E.164 numbering scheme feature is only applicable to dynamically-managed endpoint systems.

System Parameters

The CMA system operates within the following system parameters:

• Users—no limit

• Groups—no limit

• Areas—no limit

• Devices—limited to maximum number of device licenses

• Global Address Book entries—limited to maximum number of device licenses

• Room entries—no limit, but if the system has more than 500 room entries, it could experience user interface performance issues.

• Site entries—supports up to 500 total sites

• Subnets—supports up to 5000 total subnets

• Site links—no limit

Installation and Upgrade Notes

Installation of new CMA systems is managed through Polycom Global Services. For more information, please contact your Polycom representative.

If your system is not currently at v6.0 or greater, you must perform interim upgrades and apply a Pre-Upgrade Patch (Patch 9), before upgrading.

The CMA system v6.2.5 upgrade package includes the XMPP keystore patch.

Here are the upgrade scenarios that you may need to consider and apply:

Current Version	Intermediate Upgrade	Intermediate Upgrade	Intermediate Upgrade	Intermediate Upgrade	Intermediate Upgrade
5.0	→ 5.3	→ 5.5	→ Patch9*	→ 6.0*	→ 6.2.5
5.3 or 5.4	→ 5.5	→ Patch9*	→ 6.0*		→ 6.2.5
5.5.x p2 or greater	→ Patch9*	→ 6.0*			→ 6.2.5
6.0.x or 6.2.x					→ 6.2.5
* An immediate upgrade to the next intermediate software version is required.					

> ⚠️ **IMPORTANT** If in your environment, RealPresence Group Series room telepresence systems have already registered with the CMA system v6.0.x (or earlier) gatekeeper, delete them from the CMA system just before you upgrade to CMA system v6.2.1. Then once the CMA system has been upgraded, allow them to re-register. Otherwise, the Group Series systems may each consume two licenses and the data reported for them may be inconsistent.

Carefully read these Installation and Upgrade Notes and the P*olycom CMA System Upgrade Guide* for each intermediate upgrade you must perform.

IMPORTANT NOTES

- The CMA system upgrade script now verifies the system being upgrades is at a system version level that may be upgraded.
- If your system uses an internal database and one of the Pre-Upgrade Patch scenarios is required, you will also be required to perform an interim system backup after applying the Pre-Upgrade Patch. Then after upgrading the system you will perform a system restore of that backup to the CMA system v6.0 before continuing the upgrade path.
- If your system uses an external database, you will be required to perform a backup which you can then restore when the upgrade to CMA system v6.2.3 is complete.
- During the upgrade process, the system will find all RealPresence Mobile client records for clients running version lower than 1.0.3 and remove them from the system. If any of these clients are scheduled for a future conference, they will be removed from the conference. After the client is removed as a participant, if the conference has less than two participants, the conference will be removed as well.
- If the CMA system is integrated with a Polycom VBP system, we recommend shutting down the VBP system before upgrading the CMA system. Once the CMA system is upgraded, restart the VBP system.

Web Interface System Requirements

The following table describes the requirements for the CMA system v6.2.3 web interface.

Product	Versions
Microsoft Windows Operating System	2003 SP2, XP SP3, Vista™ SP2, or Ultimate 7 edition (32 and 64 bit)
Internet Browser • Microsoft Internet Explorer OR • Mozilla Firefox OR • Apple Safari	v6.0, 7.0, 8.0, or 9.0 v3.5 or 3.6 v3.2, 4.0, or 5.0
Adobe Flash Player	v9.x or 10.x

Products Tested with This Release

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

IMPORTANT

• You are encouraged to upgrade all of your Polycom systems with the latest software.

• Releases of Polycom infrastructure and endpoint systems that occurred after August 2013 may not have been tested with the CMA system. If you will be upgrading your Polycom infrastructure or endpoint systems with current releases:

➢ Consult the Current Interoperability Matrix on the Polycom support site for product support information.

➢ Consider migrating your CMA system to a Polycom RealPresence Video DualManager or RealPresence Resource Manager system.

♦ To migrate to RealPresence Resource Manager system, click here.

♦ To migrate to RealPresence Video DualManager 400 system, click here.

Polycom Products	Tested Versions
Video Endpoints	
Polycom RealPresence Group Series	4.1.1
Polycom V and VSX Series	8.7.1, 9.0.5, 9.0.6.
Polycom HDX systems	3.0.1, 3.0.3, 3.0.5, 3.1.0, 3.1.1
Polycom CMA Desktop for Windows	5.2.3, 5.2.4
Polycom CMA Desktop for Mac OS	5.2.3, 5.2.4
RealPresence Telepresence m100	1.0.4

Polycom Products	Tested Versions
RealPresence Desktop	2.3
RealPresence Mobile-iPad2®	2.1, 2.2, 2.3
RealPresence Mobile-Samsung Galaxy™	2.1, 2.2, 2.3
RealPresence Mobile-Moto Xoom™	2.1, 2.2, 2.3
Polycom ViewStation SP/MP/512	7.5.4 (H.323 only)
Polycom ViewStation FX/EX/4000	5.1.2, 6.0.5,
Polycom PVX	8.0.2
Polycom QDX 6000[a]	4.0.1
Polycom VVX 1500	UC 3.3.0, 3.3.1
Network Devices	
Polycom RMX 1500	7.8
Polycom RMX 2000	7.8
Polycom RMX 4000	7.8
Polycom MGC	9.0.4.3, 9.0.4.4
Polycom DMA 7000	5.0.1, 5.1, 5.2
Polycom VBP 5300/6400 E/S/T	9.1.5.3, 11.2.3, 11.2.5

a. Polycom QDX 6000 endpoints and Polycom DMA systems are supported only as H.323 devices.

IMPORTANT Do not use CMA systems as the gatekeeper or management system for a RealPresence Collaboration Server 800s. The CMA system has not been tested as a gatekeeper and *does not* provide management, scheduling, or monitoring capabilities in a RealPresence Collaboration Server 800s environment.

Also note that CMA systems do not support any kind of SVC/SIP functionality.

Third-Party Products	Tested Versions
Avaya One-X Communicator	6.1.1.02-SP2-33124
Avaya Communication Manager (H.323)	5.02.1.016.4 Patch18111
Cisco CTS	1.7.0.2 1.7.4
Cisco CTMS	1.7.2
Cisco CUCM	8.5.1
Cisco CUVC	7.2

Third-Party Products	Tested Versions
Tandberg MXP 550	F9.0.2 NTSC
Tandberg MXP 770	F8.2 NTSC, security
Tandberg MXP 880	F8.2 NTSC, security F9.0
Tandberg MXP 990	F9.0.2 NTSC
Tandberg MXP 6000	F9.0
Tandberg MXP 1700	F9.0
Tandberg T 150	L5.1.1
Tandberg 150 MXP	L6.2
Tandberg 6000	E5.3 B10.3
Tandberg E20	TE2.2.0.215697
Tandberg C20	TC2.0.0.191232 TC3.1.1.220240 TC3.1.2.227244 TC4.1.0.247017
Tandberg C40	TC3.1.1.220240 TC4.0.1.240265
Tandberg C60	TC3.1.1.220240 TC3.1.3.234045
Tandberg C90	TC3.1.1.220240 TC3.1.3.234045 TC4.1.0.247017
Tandberg Edge 75	F8.1 NTSC
Tandberg Edge 85	F8.2 NTSC, security
Tandberg Edge 95	F9.0.2 NTSC
LifeSize Room	4.7.0.19 4.7.11
LifeSize Room 200	4.5.1 4.7.0 4.7.0.19
LifeSize Express 220	4.7.0 4.7.0.19
LifeSize Team 200	4.7.0 4.7.0.19

Third-Party Products	Tested Versions
LifeSize Team 220	4.7.0 4.7.10 4.7.0.19
LifeSize Express 200	4.7.0 4.7.0.19
LifeSize Express 220	4.7.0.19
IBM Lotus Notes (for Polycom Scheduling Plugin[a])	8.0.2 on Windows XP (32 bit) with SP3
Microsoft OCS 2007 R2 SP0	3.5.6907.0
Microsoft Lync 2010 SP0	4.0.7457.0
Microsoft OC 2007 R2 Client	3.5.6907.0
Microsoft Lync 2010 Client	4.0.7577.0
Microsoft Exchange 2007 R2 SP3	8.3 build 83.6
Microsoft Exchange 2010 SP0	14 build 39.21
Microsoft Outlook (for Polycom Scheduling Plugin)	2007 (12.0.6557.5001) SP2 MSO (12.0.6554.5001) on Windows XP (32 bit) with SP3, Windows 7 Enterprise (32 bit) with SP1 2010 (14.0.5128.5000) on Windows XP (32 bit) with SP2, Windows 7 Home Edition (32 bit) with SP1
Microsoft Windows 2003 Server	x64 R2 with SP2 and KB updates.
Microsoft SQL Server[b,c,d,e]	2005 SP3, Standard or Enterprise edition, 32 or 64 bit 2008, Standard or Enterprise edition, 32 or 64 bit Clustering supported.
Microsoft Active Directory[f]	2003 Domain Functional Level w/ Domain Controller Windows Server 2003 SP2; multiple domain controllers 2008 Domain Functional Level w/ Domain Controller Windows Server 2008; multiple domain controllers

a. The Polycom CMA system includes a "shipped version" of the Scheduling Plugin for IBM Lotus Notes and Scheduling Plugin for Microsoft Outlook. This "shipped version" is the plugin version that has been tested and is certified to interoperate with the associated CMA system.

b. Microsoft SQL Server is required for all redundant Polycom CMA 5000 systems and for Polycom CMA 5000 systems supporting more than 400 concurrently registered endpoints and 240 concurrent calls.

c. For installations with an external database, the Polycom CMA system is only certified with the Microsoft SQL Server set to US-English Collation (SQL_Latin1_General_CP1_CI_AS).

d. The Polycom CMA system databases should have their own database instance and should not be part of a shared database instance.

e. The recommended size for the external Polycom CMA `ReadiManager_db` system database is now 4GB rather than 2GB with Autogrow set as preferred.

f. Microsoft Active Directory–Must have Global Catalogs enabled, universal groups defined, and Digitally sign communications enabled.

Polycom DMA 7000 System Interoperability

Beginning with version 4.0, the Polycom DMA system includes Call Server functionality (H.323 gatekeeper and SIP proxy/registrar), and that functionality is always enabled. A DMA system v4.0 or greater can no longer register with a CMA system as previous versions did. Instead, you should add the DMA system as a trusted neighbored gatekeeper.

In some circumstances, each call into a conference hosted on an RMX system may use two CMA system licenses. This happens when the RMX system is registered with both a CMA system and a DMA system, and the DMA system is also registered or neighbored with the CMA system. One license is consumed when the CMA system passes each call to the DMA system. The second license is consumed when the RMX system registers each call back to the CMA system. To resolve this issue, unregister the RMX system from the CMA system.

Polycom RMX Platform Interoperability

A system administrator must plan carefully when integrating a Polycom RMX conferencing platform with a CMA system as both systems manage conference settings and templates.

Synchronization of Templates and Profiles

The CMA system administrator must manually synchronize the settings in the CMA system conference template and its associated RMX profile.

Refer to the *Polycom CMA System Operations Guide* for more information on creating new conference templates. Refer to the *Polycom RMX Administrator's Guide* for more information on creating RMX profiles.

Management of MCU Ports

If you're using a CMA system, do all scheduling and monitoring through it to avoid resource conflicts. While an MCU may have on-board scheduling capabilities, scheduling conflicts can occur when both the CMA system and MCU are used simultaneously to manage the same MCU ports.

Feature Integration

Fixed and Flexible Resource Capacity Modes

The CMA system supports Polycom RMX systems operating in Flexible Resource Capacity™ mode only. The CMA system does not support RMX systems operating in Fixed Resource Capacity mode. That means that when a RMX system registers with the CMA system for the first time, the CMA system queries the RMX system for its defined number of available ports and saves this port count in a CMA system database as the RMX system's maximum capacity. The CMA system schedules, allocates, and reports port usage based on this initial value no matter how the RMX system port usage is defined or redefined.

Auto-extend Conference

The RMX system has an "ENABLE_AUTO_EXTENSION" flag that, when set, allows conferences running on the RMX system to be automatically extended as long as there are participants connected. The CMA system does not recognize this setting, so the CMA system will end a conference scheduled through it regardless of the value of this flag.

Strategic Global Partners - Cisco and Avaya Interoperability

Polycom partners with the leading platform providers—to ensure co-development and interoperability in many environments and to deliver a high quality collaborative experience. For that reason, the CMA system has been qualified to neighbor with versions of the Cisco IOS® Software Gatekeeper and the Avaya Communications Manager.

The CMA system can route H.323 calls to neighboring regions managed by the Cisco IOS or Avaya CM gatekeeper. To enable call routing to these neighboring gatekeepers, you must create CMA system dialing rules. (For more information about dialing rules, see the *Polycom CMA System Operations Guide*.) Then, if the CMA system is unable to resolve a dialed address for a call, from its list of directly registered endpoints, the system invokes the appropriate dial rule to identify the neighboring gatekeeper to which the call should be forwarded.

The Cisco IOS or Avaya CM gatekeeper may require additional configuration to integrate with the CMA system. See the product documentation for the Cisco IOS or Avaya CM gatekeeper to determine how to configure it as a neighboring gatekeeper.

For more information about partner product interoperability, refer to the partner deployment guides.

Cisco Interoperability

The Polycom video infrastructure allows you to integrate with Cisco Unified Communications Manager infrastructure to enable common dial plans between Polycom and Cisco Unified IP phones or video endpoints, as well as to take advantage of the Cisco Unified Communications Manager monitoring capabilities. For more information about this solution, see the *Polycom Unified Communications for Cisco Unified Communications Manager Environments*, which is available on the Polycom support site.

Localization Information

The CMA system user interface (UI) is available in the following languages: English, French, German, International Spanish, Japanese, Korean, Simplified Chinese, Traditional Chinese, Portuguese, and Russian.

Note that the UI may be translated for major releases only. For features delivered in minor releases that require UI changes, these UI changes may be in English only until the next major release.

Resolved Issues

The following sections include the history of issues resolved since the CMA system v6.2.0 release was first released.

Issues Resolved in CMA System v6.2.5

Issue #	Description
SSGSE-14840	The CMA system v6.0.3 is throwing an error to the CMA Desktop that says "Administrator changed the provisioning profiles. You must sign in again. The server has changed the setting for your system. The system will restart automatically."
SSGSE-14814	Endpoints could not connect to conference suddenly with ARJ reason "The reason is Max Calls Exceeded"

Issue #	Description
SSGSE-14787	In some situations, endpoints fail to register. They get a duplicate alias error.
SSGSE-14762	When the system Call Model is Direct Mode and calls come through a Polycom VBP system, the number of active calls isn't always accurate.
SSGSE-14761	The number of active calls that the CMA system allows was reached due to incorrect statistic of active calls when the CMA system interoperates with a Polycom VBP system.
SSGSE-14656	When logging in using a CMA Desktop or RealPresence Mobile client, the user experiences a duplicate alias issue.
SSGSE-14854	Endpoints were powered off and/or the network link was down during a conference. On the CMA system dashboard, they still show up as active calls number even when the conference was terminated.
SSGSE-14820	The CMA system v6.2.1 is unable to generate an Endpoint Usage Report for automatically registered TANDBERG endpoints.
SSGSE-14811	Credentials Required' alert message seen when disabling 'Common Password'.
SSGSE-14800	On v6.2.x CMA systems, there is a Scheduling/Reporting issue. When setting the "CustomizedContentRate" on the RMX system to a specific value, the CMA system Conference Usage reports are inaccurate.
SSGSE-14797	Group members disappeared from the CMA system user interface after the CMA system rebooted. This happened intermittently.
SSGSE-14791	CMA Desktop client users registering through the Polycom VBP system receive registration rejections. The rejection cause is "Full Registration Required"..
SSGSE-14694	The Polycom M100 client displays a server error when trying to register and download the Global Address Book from a CMA system running 6.2.x.
SSGSE-14673	The CMA system v6.2.2 does not fully support the RMX system v7.7.
SSGSE-14620	Multiple address books are not recognizing Groups added from Active Directory.
SSGSE-14783	The CMA system v6.2.2 adds an ISDN Dial Out Guest but does not keep the added number and the conference fails.

Issues Resolved in CMA System v6.2.4

The following table lists the resolved issues in the CMA v6.2.4 system release.

Issue #	Description
SSGSE-14802	EULA update
SSGSE-14798	CMA Desktop client failed to sign into the CMA system; the certificate date is expired.
SSGSE-14794	The CMA system can't retrieve the groups from Active Directory server if the user sets the baseDN.
SSGSE-14643	Cannot create a database migration file in some cases from CMA v6.0.1 (with patch 5) or CMA v6.2

Issue #	Description
SSGSE-14803	A "Failed to Schedule Conference" error message appears when the "Start Time" field is "Now" and the user tries to set the "End Time" field.
SSGSE-14796	SNMP: traps are not resent if the same event occurs multiple times and if the event is not cleared in system alerts.
SSGSE-14792	After upgrade to CMA system v6.2, reservation conferences do not start.
SSGSE-14782	The CMA system is not acting as a proxy for the Dell MIB traps.
SSGSE-14777	The new alert settings "Active Call Exceeded 90% of Maximum, Active Call Exceeded 100% of Maximum, E164 Alias Assignment Failed" are not documented in any CMA documentations, e.g. release notes, web online help doc.
SSGSE-14756	In some circumstances, CMA Desktop users are being unregistered from the CMA system gatekeeper when attempting to place calls.
SSGSE-14751	The MIB documentation in CMA v6.0 System Operations Guide are different from CMA v6.2 MIBs
SSGSE-14734	Customer is getting "Conference could not be persisted" errors when editing future scheduled conferences.
SSGSE-14723	A "Failed to Schedule Conference" error message appears when the "Start Time" field is "Now" and the user tries to set the "End Time" field.
SSGSE-14716	The CMA system Internet/VPN site link does not show any bandwidth utilization for Internet calls through the Polycom VBP-E system.
SSGSE-14691	Blank directory entries are displayed on Cisco Quick Set C20 endpoints after upgrading to CMA system v6.2.
SSGSE-14684	The CMA system doesn't accurately communicate when the RMX system denies a scheduled call.
SSGSE-14741	When using the Polycom Scheduling plugin for IBM® Lotus® Notes, if the client stay on the template e-mail page for more than 5 minutes, the page crashes and returns "Not responding".

Issues Resolved in CMA System v6.2.3

The following table lists the resolved issues in the CMA v6.2.3 system release.

Issue #	Description
SSGSE-14747	User with Directory Setup permission can't edit other users.
SSGSE-14743	Cannot get serial number for RealPresence Group Series 550 on the CMA system.
SSGSE-14740	RealPresence Group Series is unable to upgrade from 4.0.2 to 4.1 using the CMA system provisioning system.
SSGSE-14738	"A database error occurred while performing this action" error message when trying to delete a future conference that has been scheduled and has recurred.
SSGSE-14715	The CDR archive on the FTP server should support all the supported device types of the CMA system.

Issue #	Description
SSGSE-14698	The RealPresence Group Series produces a provisioning error for some maxTxUnitSize values.
SSGSE-14669	The CMA system is operational but connection to it via WebUI seems to be dropping every 2 minutes.
SSGSE-14665	The Groups page does not show newly added groups. Trying to open the Groups page a few times result in high memory usage alert which results in service down.
SSGSE-14641	Enable H.460 Firewall Traversal is always disabled even it is enabled in provisioning profile.
SSGSE-14395	CMA Desktop clients failed to register to the CMA system. The administrator who attempted to log into the system received failed a warning message "Initialization error, server is not ready to accept login, Please try to login shortly".
SSGSE-14730	Upgrade to CMA system v6.2.2 hotfix on KB patch failed.
SSGSE-14678	Since upgraded to CMA system v6.0.3, system alerts are not being generated when 90% of a site links bandwidth is used.
SSGSE-14677	Since upgrade to CMA system v6.0.3, site link bandwidth restrictions are working correctly but are not be reported on the topology.
SSGSE-14676	After an upgrade to CMA system v6.0.3, the Site and Site link statistic reports do not display any sites or site links.
SSGSE-14672	In some cases, on a CMA 4000 system, the memory and CPU utilization spike, the enterprise directory loses connection, and all of the groups disappear.
SSGSE-14647	Enabling the Directory Setup permissions for a role allows users the permission to modify their permission levels.
SSGSE-14637	In some cases, HDX systems report their SIP registration status in a way that causes the CMA system to display "---" in place of their E164 in the alias field of the Endpoint Monitor View.
SSGSE-14634	When an HDX ISDN GW is enabled and registered to a CMA system, ISDN Guestbook Global Address Book entries do not appear in the Global Address Book .
SSGSE-14632	Mismatch CDR report. The CMA system Call Times show Start/End Date Time in GMT but Detail CDR report show CMA system local time zone (GMT+8).
SSGSE-14631	Some users may be put in a group that will not allow them to see other groups.
SSGSE-14606	In some circumstances, a CMA system email sent for a conference scheduled is missing call in information.
SSGSE-14605	The scheduling email sent to users for ISDN dial in contains the ISDN video number, instead of the Entry Queue ISDN number
SSGSE-14570	The CMA system v6.0.3 database only displays 277 local users per web interface
SSGSE-14538	The CMA system Users table is broken after the CMA system was upgraded from v5.5 to v6.0.1
SSGSE-14519	Manual cascading with the CMA system to two RMX MCUs launches conferences, but does not create a cascade link for the RMX conference.

Issue #	Description
SSGSE-14260	Error - @0@ show up when operator click on User > Users page on CMA. No user show up on the page.
SSGSE-12883	When an HDX system is used to bridge a POTS call and a call into a Meeting Room on the RMX system, a conference appears under ongoing conferences that cannot be terminated unless the CMA system is rebooted.
SSGSE-14654	Editing a future conference that includes E164 audio-only participants results in "Insufficient MCU resource" message when re-scheduling.
SSGSE-14584	After upgrading the customer's CMA system from v5.5 the CMA Desktop contact lists were lost.

Issues Resolved in CMA System v6.2.2

The following table lists the resolved issues in the CMA v6.2.2 system release.

Issue #	Description
SSGSE-14646	After an RMX system registers with the CMA system gatekeeper, the type for the gatekeeper record should be GW/MCU and it shouldn't overwrite the pre-added RMX/MGC (with type RMX) record.
SSGSE-14645	The CMA system cannot provision the SIP URI to soft endpoints (CMA Desktop/RealPresence Mobile/RealPresence Desktop) while using Active Directory user associate with available SIP address.
SSGSE-14644	The system displays a CMA Desktop Duplicate alias error.
SSGSE-14630	The CMA system incorrectly reports gatekeeper address for managed VSX and HDX systems with software release prior to 3.0 that are registered with DMA system gatekeeper.
SSGSE-14620	Multiple address books are not recognizing Groups added from Active Directory.
SSGSE-14599	In some cases, the CMA system produces inaccurate endpoint usage reports.
SSGSE-14550	An RMX conference which is set to 'Encrypt when Possible' does not show up on the CMA system Ongoing Conference list.
SSGSE-14367	Users with Scheduler only role can see all future conferences by viewing the future conferences exported excel file.
SSGSE-14365	CMA restarted unexpectedly.
SSGSE-14350	There was an external database outage after scheduled maintenance on the SQL server. The CMA system did not come up and a message indicates the server is doing a software upgrade after boot up.
SSGSE-14346	There was a connection loss on the CMA system so the system did not respond to a Ping. After a reboot, the event viewer shows that an application pop up I/O error flooded the system log.
SSGSE-14286	The CMA system v6.0 is archiving over 90 days of XMPP database files.
SSGSE-14187	In some cases, the CMA system Network Monitor view does not show the correct status of the Polycom VBP-S.

Issue #	Description
SSGSE-14144	All CMA Desktop callers outside the Polycom VBP-ST show the same name when the RMX conference is managed by the CMA system.
SSGSE-14103	Contacts in the CMA Desktop buddy list reappear despite being deleted.
SSGSE-14048	When dynamically managed endpoints (RealPresence Mobile, CMA Desktop, and HDX systems) are registered via a Polycom VBP-ST running Access Proxy, the CMA system attempts to contact the endpoints via TCP80 at the VBP-ST's Provider (LAN) IP address to do device management. Endpoints being dynamically managed should not be contacted via TCP80.

Issues Resolved in CMA System v6.2.1

The following table lists the resolved issues in the CMA v6.2.1 system release.

Issue #	Description
SSGSE-14597	Adding more than 1000 entries to a CMA system multiple address book renders the address book unusable and not visible in the Web UI.
SSGSE-14591	Group550 series only. Failed to download Bundled provisioning on CMA system.
SSGSE-14579	SNMP CMA Endpoint register/unregister (trap)
SSGSE-14578	A Remote System Name in CDR is seen as garbled characters when a remote site in RPM whose LDAP username (AD name) contains Japanese characters. **Note** When importing a CDR report file into Microsoft Excel, select the UTF-8 format during import.
SSGSE-14486	User intermittently unable to place calls via RPM clients through to CMA system, (via VBP ST).
SSGSE-14564	CMA system Scheduled provisioning profiles for TANDBERG C series, Viewstation, and Viewstation EX/FX prevent user from entering ASCII characters in gatekeeper.
SSGSE-14563	CMA system Scheduled provisioning profiles for HDX and VSX/V-series prevent user from entering '-' (hyphen/minus) character in gatekeeper field.
SSGSE-14420	CMA system v6.01 returns GAB entries as SIP if the CMA system knows their SIP URI, even if they also have H.323 dial strings.
SSGSE-14285	When scheduling a conference via a CMA system, user adds a guest and puts IP + extension. The extension is not carried to the MGC participant.
SSGSE-14622	CMA system provisioning profiles for TANDBERG C series show an Invalid Key error.

Known Issues

The following table lists the known issues found in the CMA system which are not yet fixed.

Category	Issue #	Description	Workaround
Active Directory	SSGSE-10942	After rooms are imported into the CMA system, changes made in Active Directory to room data (e.g., email address or description) are not updated on the CMA system.	Remove and re-import the room after changes are made.
Active Directory	SSGSE-11613	When the CMA system LDAP integration credentials are invalid, an error message and exception stack trace may appear in the Jserver.log log file when the CMA system tries logging in to Active Directory.	None
Active Directory	SSGSE-11934	Enterprise directory searches on Polycom HDX systems do not succeed after initial provisioning until the endpoint is rebooted.	Reboot after initial provisioning.
Active Directory	SSGSE-6077	If dynamically managed endpoints search for rooms that were created locally on the Polycom CMA system, the search results will not return anything when using cn or displayname. Room searches on the Active Directory server will work.	Search for locally created rooms by SN and SAMAccountName.
Active Directory	SSGSE-6463	If two or more users in the Active Directory have first names and last names match, the video devices for both users will be provisioned with the same LAN host name.	None
Active Directory	SSGSE-7230	If a group is created by a domain administrator and then edited by a local administrator for the CMA server, any domain users added to the group originally will be removed.	The domain administrator will need to re-add the domain users to the group.
Active Directory	SSGSE-8764	Auto-discovery for Single Sign-on fails when integrating with a Windows Server 2008 Active Directory environment with parent and child domains.	None
Conference Management	SSGSE-10517	Scheduled conferences may have slightly shorter durations than expected. Depending on the number of participants, it may take a few seconds or minutes to get the conference started. These shorter durations will be visible in the reports.	None
Conference Management	SSGSE-11372	A scheduled conference on an embedded-MCU endpoint cannot be terminated successfully on first try. The conference appears to be gone but will show up again as an adhoc conference under the name "Internal Multipoint". Subsequent termination of this adhoc conference works.	Terminate the conference again if it reappears as an internal multipoint conference.

Category	Issue #	Description	Workaround
Conference Management	SSGSE-13510	The Conference and Chairperson passcode length defaults to the maximum of 15 characters.	None
Conference Management	SSGSE-13592	When starting a conference using the Conference On Demand feature, an external participant is created in the Conference Monitoring view on the CMA system.	None
Conference Management	SSGSE-13757	Point-to-point conferences cannot be terminated on the CMA system if the two endpoints are in the Internet/VPN site.	None
Conference Management	SSGSE-13796	A guest with an H.323 Annex-O alias cannot be connected to a conference on an RMX system, if the guest's Dial Type is set as Dial In.	Either set the Dial Type for the guest to Dial Out or use the IP address or a different alias type for the guest.
Conference Management	SSGSE-13799	The Number field of a guest displays "::", when the conference is scheduled with a Polycom RMX MCU.	None
Conference Management	SSGSE-14650	In some circumstances, a single conference between two participants appears more than once in the Conference list.	None
Conference Management	SSGSE-14651	In some circumstances, a single conference between two participants appears more than once in the Conference list.	None
Conference Management	SSGSE-14652	In some circumstances, an ISDN guest's record appears twice in the Participants List (once as ISDN and once as SIP) for a conference.	None
Conference Management	SSGSE-14766	The Add Guest function in an ad hoc conference failed.	None
Conference Management	SSGSE-14865	CMA system users cannot view the RMX profile of Meeting Rooms.	None
Conference Management	SSGSE-14868	A CMA system user cannot add participants (SIP or ISDN) when managing an ad hoc conference.	None
Conference Management	SSGSE-7728	In the Conference Management page, for a conference hosted on a Polycom RMX v 6.0 bridge with multiple ISDN participants, one of the participant details may display "Unknown."	None
Conference Management	SSGSE-7878	The Polycom CMA system does not send an email alert to the administrator or scheduler if a scheduled conference fails to launch.	None
Conference Management	SSGSE-8996	Extending the duration of a conference by 5 minutes only adds 2 minutes to the conference.	None

Category	Issue #	Description	Workaround
Conference Monitoring	SSGSE-11371	When a device is assigned to both a user and a guest, Conference Monitoring will show the guest name as the participant name when the device is connected in a conference.	None.
Conference Monitoring	SSGSE-12750	If a scheduled call was active when the CMA system was in the process of being upgraded, after the upgrade, the call may still exist on the Conference Monitoring page.	Terminate the point-to-point call from the Ongoing conference page.
Conference Monitoring	SSGSE-13288	The CMA system displays two conference participants for the same endpoint, if the endpoint registered to the CMA system after it was already connected as an external participant in a point-to-point call. The initial external participant does not get matched and updated as the registered participant while the conference is running.	Register the endpoint to the CMA system gatekeeper before the call.
Conference Monitoring	SSGSE-13578	When dialing into an entry queue on an RMX or MGC system from an endpoint using a dial string that has the bridge prefix and entry queue number, an external participnat could be created in the Conference Monitoring view on the CMA system.	None
Conference Monitoring	SSGSE-13631	TANDBERG-only multipoint calls scheduled on the CMA system and using an RMX system show extra conferences in the Conference Monitor page.	None
Configuration	SSGSE-11159	When an administrator first enables IPv6, the initial IPv6 address input by the user (in the CMA network setup) becomes the "SLAAC" address. The SLAAC address can't be removed from the system from that point on. If the administrator then changes the IPv6 address (in CMA network setup), the CMA system will then end up listening on two addresses: the SLAAC address and the new address. From then on, any time the administrator changes the address in CMA system, the second address will change, but the SLAAC address will remain. This is a Windows limitation that has no known workaround.	
Configuration	SSGSE-11363	The CMA system logs may not display timestamps using the time zone configured for the system, if the system has not been rebooted since the time zone was changed. This is an issue during out-of-box setup because there is no reboot after the time zone is set.	Reboot the CMA after changing the time zone.
Configuration	SSGSE-8995	On a Russian-SKU CMA system, the AES Encryption option is still enabled on VSX and HDX endpoints, after provisioning the Security page to disable it.	None

Category	Issue #	Description	Workaround
Database	SSGSE-13094	Legacy (v4.0 or earlier) CMA system database fields store time in local time.	None
Database	SSGSE-14269	The system database may disconnect after patching.	None
Database	SSGSE-14418	If the password for the default CMA system databse user plcmdbo is changed, and then the system is upgraded, the system will not be able to re-integrate with the external database after the upgrade. The password for the plcmdbo user on the external and the internal database must match.	Change the password for the default plcmdbo user on the external, internal, or both databases, so they are the same. Then re-integrate with the external database server.
Database	SSGSE-14655	The Restore Database function failed when the backup archive file contains HDX touch control software packages.	None
Device Management	SSGSE-10420	If an dynamically managed endpoint is rebooted after having a credentials failure, the endpoint will not reboot and not give an error message.	None.
Device Management	SSGSE-10744	A dynamically-managed endpoint may not be associated with a user for short periods of time. These issues resolve themselves in an hour or so. This happens if you delete the endpoint from the the CMA system. After approximately 5 minutes, the endpoint attempts to register with the CMA system gatekeeper (assuming it was provisioned to point to the CMA system as its gatekeeper and the CMA system is configured to "Allow all registrations." In this case, the endpoint will be added to the system without being associated to the correct user. This will resolve itself after the next provisioning cycle (typically within an hour). However, current device state (like presence status) may not be correct.	To avoid this problem, turn off an endpoint before deleting it. To resolve this problem, reboot the endpoint.
Device Management	SSGSE-11409	If, in the CMA system, you have a room in Active Directory that you first associate with an endpoint before you designate it as a room, the room will lose its association with the endpoint.	Do not associate rooms with endpoints until you have designated them as rooms.

Category	Issue #	Description	Workaround
Device Management	SSGSE-12679	If a DMA system is manually added to the CMA system (Network > Add > DMA) with a valid prefix (i.e., a prefix that has been setup on the DMA system), without adding CMA as the gatekeeper for the DMA system, the CMA system cannot display the DMA node information in the Node list.	None
Device Management	SSGSE-12999	On the Network Device > Montior View page, an RMX system may show an invalid time for the last time it was registered to the gatekeeper.	None
Device Management	SSGSE-13348	It is possible to successfully add an endpoint to the CMA system through the Global Address Book that will not be updateable.	Have the default alias be less than 64 characters.
Device Management	SSGSE-13349	If an endpoint is added through the Global Address Book and that endpoint has no aliases, the CMA system will generate an alias for it based on its name. But when the device record is updated based on what was in the Global Address Book (which still has an empty device list), the generated alias is immediately deleted.	None
Device Management	SSGSE-13669	The CMA system does not honor the priority of MCU services which results in incorrect MCU services being used for conferences.	None
Device Management	SSGSE-13682	The MCU service priority is not updated after clicking Update on the Edit MCU Service window.	None
Device Management	SSGSE-13748	During an upgrade, the softupdate files are not preserved but any schedules for softupdates are preserved. After the upgrade, whenever the scheduled softupdate happens, the softupdate will fail.	Perform all softupdates before the upgrade or wait until after the upgrade to schedule softupdates.
Device Management	SSGSE-14693	The CMA system licences release is set to 1 day but expired CMA Desktop and RealPresence Mobile clients are not released.	None
Dial Rules	SSGSE-13758	The CMA system gatekeeper does not apply dial rules when forwarding location requests to neighbored gatekeepers. If dial rules were set to add/remove some digits when calling the destination number of a remote device (not directly registered with the CMA system), the CMA system does not modify the destination number before sending the request to its neighbor gatekeepers.	Avoid dial rules that modify the destination dial string for remote devices.

Category	Issue #	Description	Workaround
Documentation	SSGSE-14105	After applying the backup patch, when the user logs out, he cannot log back in. This should be documented.	None
Documentation	SSGSE-14858	Unable to configure the suggested Auditor Best Practices	None
First Time Setup	SSGSE-12841	Cannot use the Identity Certificate Chain during First Time Setup.	None
First Time Setup	SSGSE-7476	During first time setup, if the window session times out, the first time setup will not complete and you may be required to start from the last page you were on. If the last page was the Network Setup page, the information you may have entered will be lost and you will be required to re-enter the information.	Click OK in the time-out message dialog box and as prompted, start the setup again.
Gatekeeper	SSGSE-13162	In the situation where an Avaya ACM is neighbored to a CMA system, if a call is placed from an endpoint registered to the ACM, a LocationRequest (LRQ) is sent to the CMA system. In the case where the CMA system cannot resolve the destination but does have a another neighbor, the LRQ cannot be forwarded because the ACM Location Request does not have a hopcount. The CMA system gatekeeper requires a hopcount in all LRQ messages to prevent signaling loops. This causes the call to fail since the destination cannot be located.	None
Gatekeeper	SSGSE-3623	If the Polycom CMA system gatekeeper is setup in direct mode, ad hoc point-to-point calls cannot be terminated at the Polycom CMA system.	None
Global Address Book	SSGSE-14862	Multiple address books (MAB) and tiers should not be added to Group members.	None
Global Address Book	SSGSE-7701	If you delete a standard managed device (any device that is not being dynamically managed) that is registered to the Polycom CMA system for gatekeeper, Global Address Book, and management services and then add it back (either manually or automatically), the Global Address Book status will be mismatched between the Polycom CMA system and the endpoint.	Power cycle the endpoints.
Guest Book	SSGSE-11407	Audio-only dial-out entries display incorrectly in the CMA system Guest Book. This is a label discrepancy. The label in the Join Mode column should read "Audio Only".	None
Interop-CMAD	SSGSE-10160	When a CMA Desktop software update is cancelled, it may still show as in-progress.	None

Category	Issue #	Description	Workaround
Interop-CMAD	SSGSE-11287	A "Presence Status Unknown" error is always displayed for the Polycom CMA Desktop for MacOS.	Since the CMAD Mac does not support presence, the warning may be safely ignored.
Interop-CMAD	SSGSE-14760	In some circumstances, special character that are part of a user ID entered at a CMA Desktop client and then saved as a Favorite are not displayed.	None
Interop-CMAD	SSGSE-6891	The Polycom CMA system reports a successful softupdate status of the Polycom CMA Desktop client before the update process completes on the device.	None
Interop-DMA	SSGSE-7278	When a Polycom DMA system is integrated with the Polycom CMA system, the CMA system does not display the serial number of the DMA device.	None
Interop-Endpoint	SSGSE-10017	For LifeSize Express endpoints, provisioning the properties "Video Dialing" and "Voice Dialing" will fail for certain values.	When setting up a provisioning profile to be used on a Lifesize Express, verify that the values selected for these fields are applicable to the endpoint.
Interop-Endpoint	SSGSE-10669	If a LifeSize endpoint attempts to register to a specific gatekeeper and the gatekeeper ID does not match the CMA system gatekeeper ID, the registration will fail.	Keep the gatekeeper ID blank on the endpoint or use the same ID as the CMA gatekeeper ID.
Interop-Endpoint	SSGSE-11402	The TANDBERG MXP phonebook has an issue processing entries that contain an apostrophe. If any of the entries on the page being displayed includes an apostrophe, the page is not displayed. So if page 1 has 15 entries with no apostrophes, the page is displayed. If page 2 has an entry that includes an apostrophe, it is not displayed. If page 3 has 15 entries with no apostrophes, the page is displayed.	Do not include apostrophes in the names of devices, users, guests, or rooms.
Interop-Endpoint	SSGSE-11797	When a CMA system Guest Book entry includes an extension, the guest's entry is displayed in the phone book on LifeSize endpoints with no Video Number.	None

Category	Issue #	Description	Workaround
Interop-Endpoint	SSGSE-12753	If a customer uses peripherals before upgrading to CMA system v5.5; they must force a reboot of the endpoint after upgrading to CMA system v5.5 for the peripherals to show up on the Peripherals View.	Reboot the endpoint.
Interop-Endpoint	SSGSE-13642	The CMA system shows directory status for an HDX system based on the receipt of an LDAP status event. This is a one-time event at the time the HDX system boots. If CMA system misses the event, is rebooted, or if the HDX system is provisioned without requiring a reboot (if name does not change), the CMA system may miss the event.	None
Interop-Endpoint	SSGSE-13644	The Synchronize Endpoints action fails when the Global Address Book is configured on a TANDBERG endpoint.	None
Interop-Endpoint	SSGSE-13689	Guests with ISDN endpoints show up in the LifeSize phonebook with blank values.	None
Interop-Endpoint	SSGSE-13716	The length allowed by the CMA system in provisioning HDX system passwords does not match what is implemented on the HDX systems locally.	None
Interop-Endpoint	SSGSE-14471	The details of an HDX system peripheral device cannot be viewed when the HDX system is in a call.	None
Interop-Endpoint	SSGSE-14496	The RealPresence Desktop client may request provisioning from the CMA system while it is in a call. The CMA system will fulfill that request.	None
Interop-Endpoint	SSGSE-14500	Users with more than one active RealPresence Desktop device instance may not be able to be scheduled into a conference.	None
Interop-Endpoint	SSGSE-14568	Adding multiple aliases of the same type (E164, Annex-O or H323-ID) for an endpoint system can result in multiple entries appearing in the pull down for selecting the alias. Only one of the aliases is used (most probably the first in the list for that type) and the other alias values are unavailable for selection.	None
Interop-Endpoint	SSGSE-14769	An extra point-to-point (P2P) conference was found when the endpoint join the conference using the RMX signal IP plus the conference ID.	None
Interop-Endpoint	SSGSE-14848	In some situations, a phone does not register with its new E164/H323 ID after changing the values from Endpoint Settings menu.	None
Interop-Endpoint	SSGSE-14855	In some situations, RealPresence Desktop and CMA Desktop clients lose dynamic designation and registrations do not time out and clear.	None

Category	Issue #	Description	Workaround
Interop-Endpoint	SSGSE-6088	The Polycom CMA system Device List may display the incorrect software version for Polycom ViewStation FX endpoints or the software version displayed may change inappropriately.	None
Interop-Endpoint	SSGSE-7289	The TANDBERG 6000 E is unable to send H.239 content in H323 calls when it is registered to the Polycom CMA system. The endpoint also stops transmitting video when this occurs.	None
Interop-Endpoint	SSGSE-7416	When logging into CMA Desktop with the local administrator account, you may receive notifications of available updates for third-party components in a CMA Desktop window. These notifications should be ignored.	None
Interop-Endpoint	SSGSE-7843	After restoring an HDX system to factory defaults, the HDX Management Server List may not include the CMA system to which the endpoint is registered.	None. This is a rare occurrence that the CMA system will correct every 100th polling cycle.
Interop-Endpoint	SSGSE-9031	The CMA system Get Serial Numbers function lists all non-T150 TANDBERG endpoints, including C-Series endpoints.	None
Interop-Endpoint	SSGSE-9982	The ViewStation FX & ViewStation EX devices can be found by using the Search Devices feature even if they have a remote password.	None
Interop-Endpoint	SSGSE-9986	For LifeSize Express endpoints, provisioning the "HD Camera 2 Moment" property will fail.	Set the property on endpoint manually.
Interop-Endpoint	SSGSE-9987	For LifeSize Express endpoints, provisioning the properties "HD Input 1 Name" and "HD Camera 1 Name" will fail.	Do not include these properties in provisioning profile that will be applied to LifeSize Express endpoints.
Interop-MCU	SSGSE-13665	The conference ID of an adhoc MCU conference is shown as "0000". The expected is "N/A".	None
Interop-MCU	SSGSE-4824	The content for scheduled conferences that are cascaded over multiple MCUs (MGCs or RMXs) is not viewable on the endpoints.	None
Interop-MGC	SSGSE-13113	Some MGC system settings on conference template cannot be mapped to an MGC system when scheduling a conference.	None

Category	Issue #	Description	Workaround
Interop-MGC	SSGSE-13553	A conference scheduled as a 10+ layout conference on an MGC system won't be launched as 10+ conference.	None
Interop-MGC	SSGSE-13783	A guest with an H.323 Annex-O alias cannot be connected in a scheduled conference on an MGC system, if the guest is set to dial-in. The call from the endpoint fails, and the guest shows as disconnected in the conference.	1) Set the guest as Dial-Out if you want it connected by Annex-O alias in the conference. 2) Use a different H323 dial type (IP / E164 / ID) if the participant is kept as Dial-In.
Interop-MGC	SSGSE-13784	When adding a guest to an ad hoc conference on an MGC system, the CMA system does not allow you to specify Dial In. Instead you must specify an IP address for the H.323 guest. The message the system displays does not accurately reflect the requested action.	1) You can configure the guest as DialOut in the CMA GuestBook, and use the prefered H323 dial type. 2) If dialin, and the user enters the correct IP value for the device the guest is associated with, the participant gets connected in the conference.
Interop-MGC	SSGSE-14648	When a scheduled MGC conference is active, the CMA system displays multiple conferences between the MGC and each participant.	None
Interop-MGC	SSGSE-14864	A CMA system user cannot view the MGC gatekeeper registration address.	None
Interop-MGC	SSGSE-7209	When a MGC-scheduled conference ends at its scheduled end time, some of the participants may be removed. Copying the conference at this time may result in a conference with an incomplete list of participants. This behavior is not seen consistently and is not seen if the conference is terminated before its scheduled end time.	MGC-scheduled conferences should be copied before they're end time (either before the conference is launched or when it's still ongoing).
Interop-MGC	SSGSE-9008	The Extend Duration function does not work on a scheduled conference that uses a Polycom MGC system as the bridge. The call will end at the originally scheduled end time.	None

Category	Issue #	Description	Workaround
Interop-RMX	SSGSE-14459	The DNS name for an RMX system is not automatically populated into the CMA system device screens when the RMX system is added to the CMA system.	None
Interop-RMX	SSGSE-14658	When an RMX 2000/4000 with an MPM+ card is registered with a CMA 4000, in the H.323 tab of the IP Network Service properties the ID is represented by black diamond characters with question marks inside them.	None
Interop-RMX	SSGSE-14753	The CMA system sometimes sends the wrong ISDN number to the RMX system when scheduling a mixed conference.	None
Interop-RMX	SSGSE-14755	The CMA system does not correctly handle the ISDN entry queue that comes from the RMX system.	None
Interop-VBP	SSGSE-14752	Ad hoc calls through the Polycom VBP system failed when using H323 IDs.	None
Interop-VBP	SSGSE-14763	When scheduling a conference, the endpoint information for endpoints that signed in through a Polycom VBP system is not accurate.	None
Interop-VBP	SSGSE-6544	VBP appliances that are added by the gatekeeper can be added without the Provider-side IP.	Edit the VBP appliance record. If the Provider-side IP changes, delete and re-add the VBP appliance.
Interop-VBP	SSGSE-6752	Polycom VBP appliances cannot be added to a CMA system when the system gatekeeper is set to "Allow predefined endpoints only".	The current workarounds are: (a) Take the gatekeeper out of predefined mode, add the VBP appliance, and then set it back or (b) define the VBP appliance to the gatekeeper before adding it.
Interop-VBP	SSGSE-6827	The Polycom VBP system consumes one license.	None
Interop-VBP	SSGSE-7181	A Polycom CMA Desktop client that is accessing the network through a Polycom VBP appliance gets disconnected from presence service after few hours of successful sign in.	Re-login.

Category	Issue #	Description	Workaround
Interop-VBP	SSGSE-8925	The CMA Desktop Chat icon is disabled in the call window with some Polycom VBP and Polycom CMA system settings.	None
Interop-VSX	SSGSE-6584	When a Polycom CMA system loses connection to a Polycom ViewStation FX endpoint, the CMA system reports the disconnection in the UI. However, an email alert is not generated for this connection error.	None
Localization	SSGSE-13632	The headers show in English on exported reports when CMA system is set to other language	None
Localization	SSGSE-6715	The calendar popup for scheduling a software update and for adding a conference are not localized.	None
Localization	SSGSE-6732	In non-English languages, the Delete button on the Admin > Dial Plan and Sites > Sites > Edit > Subnets web page may be truncated.	None
Localization	SSGSE-6733	Default font size is 11 pt, however this font size is unreadable for Asian languages.	End users can over-ride the default font size for their web browsers.
Localization	SSGSE-7596	If the font size is changed for a language other than English, the change does not take effect immediately.	Log out, close the browser, and start a new browser session.
Logging	SSGSE-13378	The log for the conference launch process for point-to-point calls reports a device managed state of false. This is not necessarily true but can be safely ignored.	None
Logging	SSGSE-14748	In some circumstances, the "recording time" in the logs is incorrect.	Reboot the CMA system.
Logging	SSGSE-8626	String or binary data in the EXXX_LOG is truncated.	None
Messages	SSGSE-13347	The error message that the CMA system interface posts when an attempt to delete all aliases from a device is more alarming than it needs to be.	None
Messages	SSGSE-13542	The CMA system returns a 500 error when a CMA Desktop system tries to log in with the wrong credentials. It should return a 401 error response when the username or password is incorrect.	None
Messages	SSGSE-13672	There is a Help button on a message box, but context-sensitive help can only be tied to dialog boxes, not the error messages.	None

Category	Issue #	Description	Workaround
Messages	SSGSE-5773	Scheduling failure message states 'Insufficient MCU Resources" when the problem is really "Insufficient Bandwidth".	None
Other	SSGSE-11012	By default the Administrators group owns objects created by members of the Administrators group. Tthe default owner should be the object creator.	None
Other	SSGSE-13287	Permission labels for roles are misleading. For example, Device Admin has only "Monitoring" permissions, but can do other actions and operators can monitor conferences, endpoints, and MCUs, but don't have monitoring permissions.	None
Other	SSGSE-13463	Microsoft Internet Explorer v8 has a known defect when attempting to download a file from the CMA system.	See http://support.microsoft.com/kb/824598 for the patch to IE8
Other	SSGSE-13524	The CMA system may split ISDN conference participant into multiple participants.	None
Other	SSGSE-13656	Local room User IDs are listed in the Area members list, but are not very helpful. Rooms do not have User IDs. A random value is shown.	None
Other	SSGSE-14233	The recording link may get disconnected unexpectedly after 20 - 30 minutes of connection in a Microsoft Office Communicator System R2 environment.	None
Other	SSGSE-14255	Disk space growing on Partition E due to large log files - need method to clean up old logs (especially mod_jk.log - which is now at over 5 GB and growing).	Delete or truncate mod_jk.log when it reaches large size - suggest 2 or before it reaches 5 GB.
Other	SSGSE-14262	All currently-applicable KB's from MSFT need to be available for customers to apply.	None
Other	SSGSE-14458	Upload action failed on the management system with Google Chrome browser.	None
Other	SSGSE-14505	Deleted Active Directory room records will display within the CMA system room list with the name field blank.	None

Category	Issue #	Description	Workaround
Other	SSGSE-14554	The CMA system cannot terminate point-to-point and embedded conferences if they are not managed by a gatekeeper. However, in scheduled conferences, this check is unnecessary, since the CMA system can terminate the conference using the endpoint functionality instead of gatekeeper functionality.	None
Other	SSGSE-14754	The call time records for ad hoc calls are sometimes wrong in the CDR.	None
Other	SSGSE-14757	In some circumstances, a user who is not included in an address book that is provisioned to an HDX system, still appears on the HDX system.	None
Other	SSGSE-7428	Users cannot search for rooms created locally on the CMA system by H.350 common name, given name, or display name.	None
Other	SSGSE-8090	An Area administrator can see all call detail records and all conference reports for the system.	None
Other	SSGSE-8205	The administrator needs all of the endpoints from a specific area to be usable by all users of the system without intervention.	Each user can use only those devices in his/her managed area. For all users to see devices in area "A" either all users must manage area A or all endpoints in area A must be moved to the "None" area
Polycom Scheduling for IBM Lotus Notes	SSGSE-6500	If a calendar event in the past is selected for editing, the Polycom CMA system displays a message saying that the event occurred in the past. However, the warning message should not appear at that time. Instead it should appear when the user clicks Save and Send Invitation for a start time in the past.	None
Polycom Scheduling for IBM Lotus Notes	SSGSE-7276	When using the Polycom Scheduling Plugin for IBM Lotus Notes, a user can't login when both HTTPS and Single Sign-on are enabled at the same time.	None
Polycom Scheduling for Microsoft Outlook	SSGSE-13482	The decline state on the Edit page for the conference is not consistent with the decline state on the View page when scheduled with the Polycom Scheduling Plugin for Microsoft Outlook.	None

Category	Issue #	Description	Workaround
Polycom Scheduling for Microsoft Outlook	SSGSE-14667	The Polycom Scheduling Plugin for Microsoft Outlook cannot connect to a CMA system when not using self signed certificate.	None
Polycom Scheduling for Microsoft Outlook	SSGSE-6531	On Microsoft Vista the Polycom Scheduling Plugin for Microsoft Outlook is not able to register two DLLs. It raises error messages. A usual source for this error is when the MSI has not been compiled for Windows Vista and/or does handle elevating user privileges required for COM component registration.	Launch MSI in administrator command prompt to solve this issue. At a command prompt, type in the path of the MSI package and Enter.
Polycom Scheduling for Microsoft Outlook	SSGSE-8839	Installing the Polycom Scheduling Plugin for Microsoft Outlook causes some Outlook instabillty.	None
Provisioning	SSGSE-13429	Scheduled provisioning for an HDX system does not allow Monitor 3 to be selected.	None
Provisioning	SSGSE-13608	In some cases, provisioning may report a failure provisioning certain fields. This only means that the fields that were reported as failing are not provisioned correctly. All other fields in the profile were provisioned successfully.	Changing the values of the fields that are listed in the provisioning log may resolve the issue.
Provisioning	SSGSE-7874	The Polycom CMA system provisions Username and Domain Username for Polycom HDX endpoints when Provision Domain Username option is not enabled on the CMA system.	None
Remote Alerts	SSGSE-7218	If after adding or editing a remote alert profile, a user clicks OK or Cancel to return to the Remote Alert Profile page, a profile is highlighted. If the user then clicks an action button (for example, Delete), the system displays an error.	First re-select the profile and then click the action button.
Reporting	SSGSE-10837	The Endpoint Usage Report appears to use the wrong end-date when filtering by date. This happens because the CDRs begin- and end-time are displayed as GMT, and the filter uses the CMA system local time. So if the call end-time for an endpoint is 6 pm local time on the 25th, it will show on the report as 1 am on the 26th (GMT). The filter is using the 6 pm time, so the CDR is displayed.	

Category	Issue #	Description	Workaround
Reporting	SSGSE-10922	Endpoint Usage reports for outbound and inbound usage identify endpoints by different names. The Outbound report identifies the endpoint by its system name, while the Inbound report identifies the endpoint by its alias.	None.
Reporting	SSGSE-11027	If an endpoint loses connection to the network during a call, the Endpoint Usage Report for the endpoint will not accurately reflect the conference end-time.	None
Reporting	SSGSE-11032	If a call spans midnight GMT, it will be appear in the Endpoint Usage Report as two conferences.	
Reporting	SSGSE-11923	Call Device Record (CDR) times for the start and end of calls are incorrect.	None
Reporting	SSGSE-13589	On the Endpoint CDR Report page, if an endpoint has calls that failed (wrong number, not answered, etc) the Summary tab will not show those calls in the number of calls, but the graph showing the call bit rates will have those calls taken into account. This resultes in a disrepancy between the number of calls in the tooltips versus the number of calls displayed at the top of the Summary tab.	None
Reporting	SSGSE-7316	The Endpoint Usage Report displays the start and end time of conferences for Polycom VVX devices incorrectly.	The CDR times can be used as a cross-reference. There is no automated workaround.
Scheduling	SSGSE-10142	Terminating a conference doesn't delete it from CMA system, so the conferernce ID is reserved even though the conference was terminated. With the introduction of the conference ID customization, the scheduler may wish to reuse the same conference ID multiple times, which will fail if the conference ID isn't released.	None
Scheduling	SSGSE-10601	When scheduling a point-to-point call on a CMA system that has no MCU configurered, changing the dial option of any of the participants will result in a scheduling failure.	Do not change participant dial options when scheduling a point-to-point call.

Category	Issue #	Description	Workaround
Scheduling	SSGSE-13426	The CMA system appears to be unable to recover from invalid conference settings when creating a new conference. In particular, the "Insufficient MCU resources" message may also be caused by mis-configured network sites, a missing path, or a full media path between sites. Changing the conference settings will not result in the conference being launched. Instead the CMA system will show the conference but will report the participants as being disconected. The RMX system will not report the conference at all.	None
Scheduling	SSGSE-14759	The text at the beginning and end of the Reminder E-mail in the E-mail setting page do not take effect.	None
Scheduling	SSGSE-14764	When schedule a cascading conference, the link status is not accurate.	None
Scheduling	SSGSE-6711	A conference cannot be scheduled to cross the start or end boundary of Daylight Saving Time. For example, if a two-hour conference is scheduled on Mar. 14, 2010 from 1:00 am to 3:00 am (GMT-6), the system shows that the conference is scheduled on Mar. 14, 2010 from 1:00 am to 2:00 am (GMT-6).	None
Scheduling	SSGSE-7553	Guests or other conference participants with both an IP address and E.164 alias land on the MCU with only the IP address.	None
Security	SSGSE-11020	User rights and advanced user rights settings do not meet minimum requirements in maximum security mode.	None
Security	SSGSE-11664	Session timeout during File Upload.	Increase the Session Timeout.
Security	SSGSE-11696	As a user I would expect the CMA system to confirm that my password has been changed before I am logged out.	None
Security	SSGSE-13550	Users do not get the option to update certificates after changing network information.	None
Security	SSGSE-13568	A CMA system in Maximum Security Mode can still log in using that same CMA system. You should only be able to log in via an external web interface.	None
Security	SSGSE-13607	In Maximum Security Mode - Terminal Services are not disabled until the second system reboot.	None
Security	SSGSE-13712	Reverting to the CMA system's self-signed certificate does not allow you to upload the previously uploaded valid certificate.	None

Category	Issue #	Description	Workaround
Security	SSGSE-13813	In maximum security mode, when the CMA system provisions a dynamically managed endpoint that is in the default site, the "Lock Port after Failed Logins" field in security settings will provision to be "Off". This is not a valid value in maximum security mode.	Edit the default site and save it. This will save it to the database with a value that is not "Off".
Site Topology	SSGSE-11679	Conferences don't show the correct site information.	As a best practice, if you make changes to the CMA system site topology, you should restart the system.
Site Topology	SSGSE-11955	Using the password rotation functionality may cause the password for the Site Topology Service to be set incorrectly. This will cause the Site Topology Service to become unavailable. Indications that this has happened are: 1) The following error appears in the Jserver.log file: ERROR|main|SiteTopologyService|(WebApplication Context_0) Unable to communicate with site topology backend within 120 seconds javax.naming.AuthenticationException: [LDAP: error code 49 - Invalid Credentials] 2) Accessing Sites on the CMA system results in an error message and no sites are defined.	A possible workaround is to rotate the passwords a second time.
Site Topology	SSGSE-12058	If a site is created, deleted, and then recreated, provisioning no longer works for devices in that site.	When creating a site, do not use the same name as a previously deleted site.
Site Topology	SSGSE-13565	The SIP bandwidth is not being used in calculations for sites.	None. Expected to be fixed in CMA v7.0.
Site Topology	SSGSE-13570	The Add Site Link screen allows the user to enter invalid combinations.	The CMA system recognizes the invalid combinations and issues an appropriate error message and allows the user to re-select the inputs.

Category	Issue #	Description	Workaround
Site Topology	SSGSE-14507	The Edit Network Cloud dialog box allows the user to give the Network Cloud a name that is already in use; however, an error is received when saving the change.	Enter a unique Network Cloud name.
Site Topology	SSGSE-6643	The new site topology map view may display clouds under sites. In some cases, the clouds can't be moved, because the site has focus. The sites can't be moved, because they are geographically fixed.	Edit the site and temporarily change the location data. Move the cloud and then edit the site and enter the correct location information.
SNMP	SSGSE-12073	In some cases, the CMA system SNMP MIB does not include all of the information that is displayed on the CMA system user interface. This issue will be addressed in a subsequent release.	None
SNMP	SSGSE-6236	SNMP returns incorrect number of total conferences.	None
SNMP	SSGSE-6307	SNMP reports on the number of ad hoc conferences is offset by one. SNMP also reports the total conferences in one day based on a 24-hour interval rather than on the actual calendar dates.	Use the Today's Ad hoc Conferences and Today's Scheduled Conferences pane on the dashboard for accurate conference information.
SNMP	SSGSE-6657	The Polycom CMA system does not always send the correct NTLM version for devices through to SNMP.	None
System Access	SSGSE-11608	When the CMA system has a session timeout during a file upload or system scan, the browser locks up.	Terminate the browser process, relaunch, log back into the CMA and try the upload again.
UI	SSGSE-10050	Some UI pages with grids do not recognize that a row is selected, so when an ACTION command is clicked, the user gets an error message saying "The set of device IDs must not be null". The set of IDs is the set of selected rows in the grid.	Refresh the browser or logout and log back in.

Category	Issue #	Description	Workaround
UI	SSGSE-10282	After finishing the uploading of the first software update on the Automatic Software Update page, the popup box that is displayed (telling the user that it will assume to be the policy for this device type) is cut off at the bottom. The cutoff text is the last part of the following message: "To modify, see the 'Version to use' section at the top of the screen."	Click OK to dismiss the popup.
UI	SSGSE-10303	If the User Interface Timeout value is set to a large number, such as 9999999, the system becomes blocked with "Your session has timed out".	To avoid this problem, do not use large timeout values.
UI	SSGSE-11198	In the "Add New Room" dialog box the participant names are cut off.	None
UI	SSGSE-11749	The text on the Reset System Passwords page doe not resize or wrap correctly.	None
UI	SSGSE-13203	The method for selecting dates for the reporting features of the CMA system user interface is inconsistent. Although this causes no real issue, it does need to be changed to make it consistent.	None
UI	SSGSE-13306	When deleting a provisioning bundle, the user must confirm the deletion and then acknowledge that the bundle was deleted successfully. In the future, the second popup for the status of the deletion will not occur if the deletion was successful.	None
UI	SSGSE-13320	When editing an endpoint (Endpoint > Monitor View > Edit), the ISDN video number could not be saved if ISDN(H.320) is not selected.	None
UI	SSGSE-13443	When scheduling a conference, if a lecturer is selected that has a long name, the page is resized so certain fields are not viewable without using the scrollbar at the bottom.	None
UI	SSGSE-13486	The CMA system does not display the correct conference lecturer when the lecturer is changed during an active conference.	None
UI	SSGSE-13681	Duplicate MCU services are displayed on the CMA system interface if a user repeatedly clicks the Update button when adding a new MCU service for an RMX system.	None
UI	SSGSE-13734	After failover, the CMA system logo on the new active server is inconsistent with the CMA system logo on the original active server.	None
UI	SSGSE-13754	The number of characters allowed in the Time Server field on the Provisioning page is not sufficient for the full DNS name.	None

Category	Issue #	Description	Workaround
UI	SSGSE-14440	The profile information is missing from meeting rooms in the MCU Network Device page.	None
UI	SSGSE-14506	There is no data validation on the E164 and IP Number data entry fields for an H.323 guest.	None
UI	SSGSE-14635	In some circumstances, the Site Statistics and Site-Link Statistics pages do not show any data.	None
UI	SSGSE-14863	The CMA system user gets a pop up error when adding an RMX system to a CMA system with a system name of "test"	None
UI	SSGSE-14870	The CMA system displays an extra conference record between RMX and participant.	None
UI	SSGSE-6109	When tabbing through the internal pages, the Views and Actions labels can be accessed, but not individual views or actions. This makes it impossible for keyboard-only users (users who can't use a mouse) to switch views or initiate actions.	None
UI	SSGSE-6530	With 500 sites + 500 links, first time access can take 3-5 minutes but the system does not indicate that something is happening.	None
UI	SSGSE-6538	If users access the Polycom CMA system web interface from a PC that has the Polycom Scheduling Plugin for Microsoft Outlook installed, they may get intermittent messages stating "Device Not found".	Uninstall the Polycom Scheduling Plugin for Outlook.
UI	SSGSE-6545	After deleting a remote alert profile, users may get an error message that indicates "Failed to delete profile", but the profile was actually deleted. This is a refresh error.	Navigate away from the page and then return.
UI	SSGSE-6796	The Conference Management page may not automatically refresh and show the correct status of a long duration call if the call disconnects by itself, especially if the disconnect occurs at or after midnight.	Click Refresh to manually refresh the page.
UI	SSGSE-7138	For some pop-up messages on the Polycom CMA system, selecting OK does not close the popup.	Click the red X to close the popup message.
UI	SSGSE-7320	When a registered MCU has calls on it, there is no far site call information in the View Details dialog box.	None
UI	SSGSE-7480	See SSGSE-7481	

Category	Issue #	Description	Workaround
UI	SSGSE-7498	Selecting the ISDN Required MCU Service on the Device Capabilities page results in a database update even if there is no change in the device information.	None
UI	SSGSE-7499	If a non-dynamically managed endpoint entry is deleted from the Global Address Book and gatekeeper and then the endpoint re-registers automatically, the CMA system will report inaccurately that its Global Address Book and gatekeeper registrations are down.	Restart the endpoint.
UI	SSGSE-7537	A IP-only VSX endpoint will be reported with a SIP alert on a CMA system even when there is no SIP registration attempt from the VSX.	None
UI	SSGSE-7552	MGC and GW/MCU device's site does not update when the device's subnet is added to a site.	Delete the GW/MCU and MGC. After re-registration the UI will display the site correctly.
UI	SSGSE-7644	View Participant Details and Device Summary screens show an unfamiliar device ID.	None. These are IDs used for troubleshooting.
UI	SSGSE-7745	When a PVX is in a conference, an administrator can select View Participant Details for it, and the View Participant details pop-up window appears and Manage Device is one of the available actions. However, Manage Device does not apply to a PVX, and selecting the option for a PVX generates an error message.	None
UI	SSGSE-7917	The Gatekeeper pane shows inaccurate counts.	None
UI	SSGSE-7926	The Internet site is no longer shown on the Site Statistics page.	None
UI	SSGSE-7977	If an ISDN line is down, the CMA system does not send an alert even though it does shows the line is down.	None
UI	SSGSE-8383	There are redundant commas in the Japanese translation of "Date and Time" information.	None
UI	SSGSE-8994	In the Gatekeeper pane of the CMA system Dashboard, Alternate Configured is always No.	None
UI	SSGSE-9030	The CMA system Device List refers to endpoint models inconsistently (specific model vs. series).	None

Category	Issue #	Description	Workaround
Upgrade	SSGSE-12682	Apple Safari or Mozilla Firefox on a MacIntosh (MAC) computer do not support the CMA system upgrade process. The file is not uploaded correctly.	Use a Microsoft Windows system with Apple Safari, Mozilla Firefox, or Microsoft Internet Explorer for CMA system upgrades.
Upgrade	SSGSE-14242	A Hot Fix applied to newer Hot Fix on same patch level wrongly succeeds.	None
Upgrade	SSGSE-14590	In some instances, upgrades to the CMA system software fail but the CMA software version data gets updated.	None
Upgrade	SSGSE-14611	On migrating from CMA system to Resource Manager system, the E.164 Alias Assignment Failed alert value is not being migrated.	None
Upgrade	SSGSE-14653	Two versions of the CMA Desktop v5.2.3.19935 clients are listed when the client is installed onto a CMA v6.0.0 system and then the CMA system is upgraded to v6.2.1.	None
Upgrade	SSGSE-7921	After upgrading the system, any devices that had two rows in the H323Address no longer get updated correctly.	None
Upgrade	SSGSE-8309	After upgrading to CMA 5.0, CMA Desktop users were added to the Global Address Book, even though the Include dynamically- managed devices in the Global Address Book was unchecked.	Enable and then disable the Include dynamically- managed devices in the Global Address Book option.
Upgrade	SSGSE-9088	Multiple MCUs lost gatekeeper registration with CMA system. PN_Log.txt stops reporting info after upgrade from v4.1.4 to v5.0.	None

The following table lists some of the known limitations of the CMA system when interoperating with partner gatekeepers and endpoints.

Issue #	Description	Comment
CSC-6	Cisco/Busy signal is heard on Cisco phones when VSX or HDX disconnects.	An endpoint issue related to issue VIDEO-57092, which is marked Will Not Fix.
CSC-3	Call Type in conference management screen indicates an incorrect type	Open issue

Issue #	Description	Comment
CSC-2 SSGSE-2200	Bit Rate in conference management screen is incorrect	Open issue
AVA-707 CSC-5 SSGSE-2202	Mute indication not displayed in conference management screen when muting occurs.	Open issue
AVA-708	Avaya/Video protocol and format on the conference management screen always displays as AUTO.	Open issue
AVA-726	Avaya/RMX2000/CDR/Destination field is blank on the CDR when the Avaya softphone or hardphone dial into a conference.	Open issue
AVA-715	No audio heard after Avaya phone is taken off hold.	Enhancement request. The CMA system does not currently support audio shuffling.
AVA-716	Endpoints do not negotiate video when the Avaya softphone transfers a call.	Enhancement request. The CMA system does not currently support audio shuffling.
AVA-709 CSC-4	Incorrect call duration for an ad hoc conference.	Enhancement request. Currently, the CMA system shows duration for scheduled conferences only, not ad hoc conferences.
SSGSE-4566	In an environment with an Avaya ACM, if a RMX registered to a CMA system has an audio call to a telepresence room, the telepresence systems will get excessive background/white noise.	Open issue

Where to Get the Latest Product Information

To view the latest Polycom product documentation, visit the Support page of the Polycom website at http://support.polycom.com

Appendix A: SQL Server Configuration to Prevent Random Database Disconnection

Polycom CMA and ReadiManager SE200 systems connected to an external database sometimes experience problems with random disconnection from the Microsoft SQL server. A subset of database connections from a Polycom CMA or ReadiManager SE200 system may drop, and a drop can remain unnoticed until a user performs an operation that attempts to use the connection. This problem is exacerbated by the fact that a Polycom CMA or ReadiManager SE200 system does not try to reconnect on its own. We have enhanced some system modules, such as the Device Manager and CDR Manager, so they do initiate a reconnection to the database, which alleviates the problem to a great extent. But there are still modules that do not.

After researching the problem, we have determined that the database connection is closed by the TCP stack on the Microsoft SQL 2005 server, not by the Polycom CMA and ReadiManager SE200 systems. There is a fairly new feature in the SQL server's TCP that looks for orphaned connections. The server sends "Keep Alive"(heartbeat) messages to the client through each of the connections and expects acknowledgments. If no acknowledgment is received within stipulated time and after a stipulated number of re-transmissions, the server closes that particular connection. The default time for "Keep Alive" message to start is 30secs. If no acknowledgment is received from the client for that particular connection, the local server TCP will keep sending "Keep Alives" to the client and will wait for KeepAliveInterval(default 1sec) between each retransmissions. After TcpMaxDataRetransmissions (default 5) times of sends-and-no-acknowledgments, the server will close the connection with the assumption that the client is probably not operational anymore.

The default setting for this feature has been found to be too aggressive and it renders easy for client systems to fatally miss successful acknowledgments every time. Temporary network latencies, systems being too busy to respond or even the low level NICs state can cause this failure.

Hence, Polycom recommends changing the configuration of the "Keep Alive" settings on the server to pace the heartbeats better. We have tested with various wait-time settings for the "Keep Alive" variable and have found that exercising this feature every hour to be ideal.

The change of configuration on SQL server is on a per instance basis. So the affect should be localized and should not affect other instances in the same database.

The following is the procedure:

1 From the Microsoft SQL Server Configuration Manager, select Start > All Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager.

2 Expand SQL Server 2005 Network Configuration.

3 Select the relevant instance. For default, select Protocols for MSSQLSERVER.

4 Double click TCP/IP.

5 Select the field that corresponds to the KeepAlive setting.

6 Type in the number of milliseconds the Microsoft SQL server should wait before sending subsequent KeepAlive messages.

   NOTE: The tested value is 3600000 (once every hour).

7 Restart Microsoft SQL server.

Trademark Information

POLYCOM® 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.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

End User License Agreement

Use of this software constitutes acceptance of the terms and conditions of the Polycom RealPresence CMA system end-user license agreement (EULA).

The EULA for this product is available on the Polycom Support page for the RealPresence CMA system.