RELEASE NOTES Version 8.6.7 | Dec 2016 | 3725-74103-000D2

Polycom® RealPresence® Collaboration Server (RMX®) 1800/2000/4000

Polycom announces the release of the Polycom RealPresence® Collaboration Server (RMX) version 8.6.7 software. This document provides the latest information about this release.

Contents

What's New in this Release

RealPresence® Collaboration Server 8.6.7 Changed Feature

RealPresence® Collaboration Server 8.6.4 Changed Feature

RealPresence® Collaboration Server 8.6.2 New Features

RealPresence® Collaboration Server 8.6 New Features

Products Tested with this Release

RMX Web Client System Requirements

System Upgrade Information

Known Issues

Resolved Issues

Get Help

Copyright and Trademark Information

What's New in this Release

This RealPresence® Collaboration Server release is a maintenance release that fixes the issues identified in the Resolved Issues section.

This release also includes the new or changed feature identified in RealPresence® Collaboration Server 8.6.7 Changed Feature section.

For customers upgrading from releases before 8.6, see the following sections for more information about the new and changed features in this software branch.

Note: New Platform Annotation
The 1800-EL annotation in the table below relates to the new Polycom® RealPresence® Collaboration Server 1800 Entry Level for Japanese market.

RealPresence® Collaboration Server 8.6.7 Changed Feature

The following table lists the changed feature in Collaboration Server 8.6.7

Version 8.6.7- Changed Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Security	TLS 1.1 and TLS 1.2	In addition to TLS 1.0, APACHE, Central singling, LDAP, EXCHANGE and ICE (TURN) are able to communicate on TLS1.1 and TLS 1.2.	Yes	Yes	Yes

RealPresence® Collaboration Server 8.6.4 Changed Feature

The following table lists the changed feature in Collaboration Server 8.6.4.

Version 8.6.4 - Changed Feature

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Collaboration	Polycom® RealPresence Clariti™ Support	RealPresence Collaboration Server 1800/Virtual Edition will be enabled with full capacity in the RealPresence Clariti solution.	No	Yes	Yes

RealPresence® Collaboration Server 8.6.2 New Features

The following table lists the new features in Collaboration Server 8.6.2.

Version 8.6.2 - New Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Certificate	New CSR guideline	A few changes to existing CSR guidelines.	Yes	Yes	Yes
IVR	Suppress Operator's Entry Tone	A new system flag.	Yes	Yes	Yes
Rest API	SNMP	Support configuring SNMP through Rest API.	Yes	Yes	Yes
Recording	RealPresence Media Suite/Capture Server Dial-In RealPresence Collaboration Server through H.323	Support recording / playback for H.323 calls.	Yes	Yes	Yes
Lync	Support for Microsoft® Skype for Business	Polycom added support for Microsoft® Skype for Business as part of Polycom products' deployment into Microsoft Environment. Note: The latest RealPresence Platform versions are required.	Yes	Yes	Yes
Audio	Disable G.729 codec through flag in favor of G.711	A system flag allows disabling G.729 is favor of G.711, when there is a requirement for higher audio quality.	Yes	Yes	Yes
Cascade	Support chairperson in cascaded conferences	The behavior of a conference with a chairperson is widened to encompass cascading scenarios. Requires supporting DMA system version.	Yes	Yes	Yes
Licensing	New CSR Guideline	New Certificate Signing Request (CSR) guideline introduced.	Yes	Yes	Yes

RealPresence® Collaboration Server 8.6 New Features

The following table lists the new features in the Collaboration Server 8.6 release.

Version 8.6 - New Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Lync					
Lync	New RealConnect topology for Lync via Service Provider. ICE over IPv4 is used to connect the RMX to AVMCU.	The Collaboration Server supports federation with Service Providers in scenarios where the RPP solution and the Service Provider reside in separate locations. This enables customers with Lync infrastructure, but no Polycom infrastructure, to invite into Lync conferences non-Lync users, where both user types may enjoy complete Lync/Polycom experience, respectively. Connection between Collaboration Server and AVMCU uses ICE over IPv4.	Yes	Yes	No
Lync	Wait for chairperson when call from RMX is in Lync AVMCU lobby	Microsoft Lync presenter is similar to chairperson behavior in Collaboration Server. The two concepts are now interacting to a consistent behavior across joined meetings. This enables conferencing stability due to possible discrepancy between Lync and Collaboration Server organizer/chairperson settings, as well as prevent unauthorized mis-usage of Collaboration Server conferencing services via the VMR created by Lync.	Yes	Yes	No

Version 8.6 - New Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Lync	RMX failover through DMA - handling Lync 2013 AVMCU connection.	Should the Collaboration Server fall during a RealConnect conference with Microsoft Lync, the DMA now maintains information on the RealConnected AVMCU, such that in addition to the previous re-establishment of the conference on an alternate Collaboration Server, the DMA also recreates the link with the AVMCU, and disconnects all its links to the original Collaboration Server.	Yes	Yes	No
Lync & Network	Lync Front End Server DNS Failover/Load Balancing	The Collaboration Server uses a new methodology to ensure Lync Front End Pool load balancing, as well as failover, through DNS.	Yes	Yes	No
Lync	Support for Microsoft® Skype for Business	Polycom added support for Microsoft® Skype for Business as part of Polycom products' deployment into Microsoft Environment. The Polycom product versions and the Microsoft® Skype for Business versions tested can be found in the Products Tested with this Release below. **Note:** The latest RPP versions are required.	Yes	Yes	No
Security					
Ultra Secure Mode	Block external VGA in CNTL board in UC APL version	In Ultra Secure Mode, the external VGA ports in Collaboration Servers 2000/4000 control boards are blocked.	Yes	No	No
Ultra Secure Mode	Lync 2013 in UC APL mode interoperability with RMX in UC APL mode		Yes	Yes	No
Ultra Secure Mode	UC APL JITC Certification for RMX1800 and MPM RX	Ultra Secure Mode platform compliance is limited now to Collaboration Servers 2000/4000 with MPMRx media cards and Collaboration Server 1800.	Yes	Yes	No

Version 8.6 - New Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Ultra Secure Mode	UC APL remove the restrictions that come with USM flag	There are some changes made to the set of Ultra Secure mode system flags.	Yes	Yes	No
Ultra Secure Mode	CRL download from CRL Distribution Point (CDP)	An automatic download of CRL (for licensing) is added to prevent malfunctioning of Collaboration Servers in Ultra Secure Mode.	Yes	No	No
Network and System					
HW	Over CPU Protection	A mechanism for detecting CPU overuse is created, to improve system robustness in overload conditions.	Yes	Yes	No
Network	OpenSSL upgrade	Some fixes of OpenSSL issues.	Yes	Yes	No
Cascading					
Cascade	Enable chairperson to manage cascaded meetings	The behavior of a conference with a chairperson is widened to encompass cascading scenarios. Involves some changes in DMA.	Yes	Yes	No
Cascade	Snatch content over cascade link	Snatching content token is now possible is cascading scenarios in addition to that of single MCU.	Yes	Yes	No
Hardware					
HW	Reset Media Card	Reset of MPMRx media cards using the Hardware Monitor.	Yes	No	No
HW	MPMx Excluded from Version 8.6	MPMx media cards is not supported from version 8.6. Some of the Collaboration Server features specific to this media card are no longer available. **Note:** Due to this change, RMX 1500 is not supported from Version 8.6.	No	No	No
HW	A new Collaboration Server 1800 Entry Level Platform	A new Collaboration Server 1800 Entry Level (EL) platform with reduced capabilities is introduced to answer the needs of small businesses in the Japanese market.	No	No	Yes
Miscellaneous					

Version 8.6 - New Features

			Platform		
Category	**Feature Name**	**Description**	**MPMRx**	**1800**	**1800-EL**
Conferencing	4x5 Layout	A simple 4x5 grid layout is added.	Yes	Yes	Yes
Conferencing	Show number of video participants	AVC participants view indication on existence and number of video participants, in addition to previous audio participants indication.	Yes	Yes	No
Licensing, SVC	Change SVC License ratio to 1:5	SVC licensing ratio is enhanced.	Yes	Yes	No
Audio	Configuration option to disable G.729	A system flag allows disabling G.729 is favor of G.711, when there is a requirement for higher audio quality.	Yes	Yes	No

Products Tested with this Release

The RealPresence Collaboration Server 1800/2000/4000/Virtual Edition systems are tested extensively with a wide range of products. The following list is not a complete inventory of compatible equipment. It indicates the products that have been tested for compatibility with this release.

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

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Gatekeepers/Proxies			
Polycom® RealPresence® Resource Manager	10.0.1	10.0.1	10.0.1
Polycom® RealPresence® Collaboration Server	8.6.7	8.6.7	8.6.7
Polycom® RealPresence® Distributed Media Application™ (DMA®)	6.4.1	6.4.1	6.4.1
Polycom® RealPresence® Access Director™	4.2.3	4.2.3	4.2.4_230053
Polycom® RealPresence® Web Suite Experience Portal			2.1.2.730_229386
Polycom® RealPresence® Web Suite Services Portal			2.1.2.265_229348
Polycom® Video Border Proxy (VBP)	V11.2.13RC2	V11.2.13RC2	V11.2.13RC2
Avaya Scopia® Serial Gateway	8.3.0.103.0	8.3.0.103.0	8.3.0.103.0
BroadWorks			AS version Rel_21.sp1_1.551
Cisco TelePresence ISDN GW 3241	2.2 (1.111)	2.2 (1.111)	2.2 (1.111)
Cisco TelePresence MCU 4505	4.5 (1.85)	4.5 (1.85)	4.5 (1.85)
Cisco 5310 MCU	4.5 (1.85)	4.5 (1.85)	4.5 (1.85)
Microsoft Lync 2013 server	5.0.8308.956	5.0.8308.956	5.0.8308.956

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Microsoft Skype for Business Server 2015 (volume license key installed)	6.0.9319.235/6.0.9319.259	6.0.9319.235/6.0.9319.259	6.0.9319.235/6.0.9319.259
Microsoft Exchange 2013	CU12 15.00.1178.004	CU12 15.00.1178.004	CU12 15.00.1178.004
Sonus Session Border Controllers (SBCs)			V05.00.02-R000
Recorders			
Polycom® RealPresence® Media Suite	2.7	2.7	2.7
MCUs, Call Managers Network Devices and Add ins			
Polycom® ContentConnect™ Server	1.5.1.196	1.5.1.196	1.5.1.196
Avaya Scopia® ISDN P10 Gateway	5.7.2.0.25	5.7.2.0.25	5.7.2.0.25
Avaya Aura® Session Manager	6.3.4.0.634014	6.3.4.0.634014	6.3.4.0.634014
Avaya Aura® Communication Manager	R016x.03.0.124.0	R016x.03.0.124.0	R016x.03.0.124.0
Cisco Unified Communications Manager	11.5.1	11.5.1	11.5.1
Cisco TelePresence Multipoint Switch	1.9.3	1.9.3	
Cisco TelePresence Server	4.2(4.18)		
Cisco TelePresence Video Communication Server	X8.8.1	X8.8.1	X8.8.1
Virtual Machines for RealPresence Collaboration Server VE Deployment			
VMware vSphere (vCenter) Client			6.0
Endpoints			
Polycom® RealPresence Debut™	1.2.0	1.2.0	1.2.0.63005
Polycom® RealPresence Trio™ 8800	5.4.4	5.4.4	5.4.4
Polycom® HDX®	3.1.11	3.1.11	3.1.11_53024

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Polycom® RealPresence® Group Series	5.2.1/6.0.0	5.2.1/6.0.0	5.2.1/6.0.0
Polycom® OTX®	3.1.8	3.1.8	
Polycom® OTX® Touch Controller	1.12.0 CTRL / 1.12.0 OS	1.12.0 CTRL / 1.12.0 OS	
Polycom® RPX®	3.1.4	3.1.4	
Polycom® VSX® and V Series Family	9.0.6	9.0.6	9.0.6
Polycom® ViewStation®	7.5.4 or higher	7.5.4 or higher	7.5.4 or higher
Polycom® ViewStation® FX/EX/4000	6.0.5 or higher	6.0.5 or higher	6.0.5 or higher
Polycom® CMA® Desktop	5.2.6	5.2.6	5.2.6
Polycom® CMA® Desktop for MAC	5.2.6	5.2.6	5.2.6
Polycom® QDX® 6000	4.0.3	4.0.3	4.0.3
Polycom® RealPresence® Mobile for Apple® iOS	3.7	3.7	3.7.0.63943
Polycom® RealPresence® Mobile for Android™	3.7	3.7	3.7.0.63943
Polycom® RealPresence® Desktop for Windows®	3.7	3.7	3.7.0.63943
Polycom® RealPresence® Desktop for Mac®	3.7	3.7	3.7
Polycom® VVX® 300/400			5.5.0.20556
Polycom® VVX® 500	5.7.0.18267	5.7.0.18267	5.7.0.18267
Polycom® VVX® 501	5.5.0	5.5.0	5.5.0
Polycom® VVX® 600	5.7.0	5.7.0	5.7.0
Polycom® VVX® 601	5.5.0	5.5.0	5.5.0
Polycom® VVX® 1500	5.5.0	5.5.0	5.5.0
Polycom® SoundPoint® IP 650	4.0.7	4.0.7	4.0.7
Polycom® SoundStation® IP 7000	4.0.11	4.0.11	4.0.11

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Polycom® Touch Control (for use with HDX)	OS1.17.0-38 / TP1.17.0-58	OS1.17.0-38 / TP1.17.0-58	OS1.17.0-38 / TP1.17.0-58
Polycom® Touch Control (for use with RealPresence Group Series)	OS6.0.0-903 / TP 6.0.0-280932	OS6.0.0-903 / TP 6.0.0-280932	OS6.0.0-903 / TP 6.0.0-280932
Polycom RealPresence touch	OS 2.0.0-193 TP6.0.0-280932	OS 2.0.0-193 TP6.0.0-280932	OS 2.0.0-193 TP6.0.0-280932
Polycom® CX5500	1.2.0	1.2.0	1.2.0
Polycom® CX8000	1.00.11.066	1.00.11.066	1.00.11.066
Avaya Scopia® XT5000	8.3.2.534	8.3.2.534	8.3.2.534
Avaya Scopia® XT7000	8.3.2.225	8.3.2.225	8.3.2.225
Avaya one-X® Deskphone	S3.171b	S3.171b	S3.171b
Avaya one-X® 1000 Communicator	6.2.10.03-FP10	6.2.10.03-FP10	6.2.10.03-FP10
Avaya 1000 Series Video Conferencing Systems	4.8.3(23)	4.8.3(23)	4.8.3(23)
Avaya Desktop Video Device	1_1_2_020002	1_1_2_020002	1_1_2_020002
Avaya Flare® Experience for iPad Devices	2.0.6	2.0.6	2.0.6
Avaya Radvision Scopia XT1000	2.5.416	2.5.416	2.5.416
Avaya Radvision Scopia XT5000	V8_3_2_534	V8_3_2_534	V8_3_2_534
BroadTouch Business Communicator for Desktop			21.5.1.1179
BroadTouch Business Communicator for iOS			22.0.1.5873(Tablet) 22.0.1.5871(Mobile)
BroadTouch Business Communicator for Android			21.2.4.5513(Tablet) 21.5.4.5513(Mobile)
Cisco TelePresence System EX90	7.3.6	7.3.6	7.3.6
Cisco TelePresence Integrator C20/C40/C90	7.3.6	7.3.6	7.3.6

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Cisco TelePresence SX10/SX20/SX80	8.2.1	8.2.1	8.2.1
Cisco TelePresence System 3010	1.10.15(4)	1.10.15(4)	
Cisco TelePresence System 1300	1.10.15(4)	1.10.15(4)	
Cisco TelePresence TX9000	6.1.12(4)	6.1.12(4)	
Cisco TelePresence TX1310	6.1.12(4)	6.1.12(4)	
Cisco TelePresence System 500-37	6.1.12(4)	6.1.12(4)	
Cisco TelePresence System 500-32	1.10.15(4)	1.10.15(4)	1.10.15(4)
Cisco TelePresence IX5000	8.1.2(12)	8.1.2(12)	
Cisco DX70 DX650	10-2-5-212	10-2-5-212	10-2-5-212
Cisco DX80	ce8.2.1	ce8.2.1	
Cisco Jabber for Windows	11.1	11.1	11.1
Cisco Jabber for Mac	11.1	11.1	11.1
Cisco TelePresence System 1700 MXP	F9.3.4	F9.3.4	F9.3.4
Cisco TelePresence System Edge 95 MXP	F9.3.4	F9.3.4	F9.3.4
Huawei TE30/TE40	2.0.200	2.0.200	2.0.200
LifeSize Icon 600	2.9.1.(2001)	2.9.1.(2001)	2.9.1.(2001)
LifeSize Express 220	5.0.9(2)	5.0.9(2)	5.0.9(2)
LifeSize Team 220	5.0.9(2)	5.0.9(2)	5.0.9(2)
Microsoft Skype for Business client (preview MSO)	16.0.4318.1000/16.0.7127.1021	16.0.4318.1000/16.0.7127.1021	16.0.4318.1000/16.0.7127.1021
Microsoft Lync Phone Edition for Polycom CX500/CX 600	4.0.7577.4487	4.0.7577.4487	4.0.7577.4487
Microsoft Skype for Business client (Android)	6.9.0.1	6.9.0.1	6.9.0.1
Microsoft Skype for Business client (iOS)	6.9.0.313	6.9.0.313	6.9.0.313
Microsoft Lync Mac client	14.3.3	14.3.3	14.3.3
Microsoft Lync 2013 client	15.0.4809.1000	15.0.4809.1000	15.0.4809.1000

Device	MCU Type		
	2000/4000	1800	Virtual Edition
Microsoft Lync 2010 client	4.0.7577.4498	4.0.7577.4498	4.0.7577.4498
Sony PCS-XG80	2.46	2.46	2.46
Sony PCS-XG100	1.60	1.60	1.60

RMX Web Client System Requirements

The following table lists the environments (Web Browsers and Operating Systems) with which the RMX Web Client was tested.

Web Browser	Operating System
Internet Explorer 7	Windows Vista™
	Windows 7*
Internet Explorer 8	Windows 7*
Internet Explorer 9	Windows 7* and Windows 8
Internet Explorer 10	Windows 7* and Windows 8
Internet Explorer 11	Windows 8.1 and above

Windows 7 Note

When using Internet Explorer 8 to run the RMX Web Client application, Protected Mode must be disabled before downloading the software to the workstation. To do this:

1. Open an IE browser window and go to Internet Options > Security tab.
2. Clear the Enable Protected Mode check box for each of the following tabs: Internet, Local intranet, and Trusted sites.
3. When the software is successfully installed, recheck the Enable Protected Mode check box for the Internet and Local intranet. Leave it disabled for Trusted sites.

Windows 8 Note

When using Internet Explorer 8 to run the RMX Web Client application, it is important to configure the browser according to the following procedure:

1. Close all IE browser windows and verify that no iexplore.exe processes are running on the system.
2. Open a new IE browser window and go to Internet Options > General tab.
3. In the Browsing history section:
   - Click Delete.
   - From the Delete Browsing History dialog box, select the Temporary Internet files and Cookies check boxes.
   - Click Delete.
4. In the Browsing history section:
   - Click Settings.
   - In the Temporary Internet Files and History Settings dialog box, click View objects.
   - In the Downloaded Program Files select the EMAClassLoader.dll file.
   - Click Delete.
5. Click OK.

System Upgrade Information

The following sections provide important information about upgrading RealPresence Collaboration Server 1800/2000/4000 systems to this release.

Important Upgrade Notes

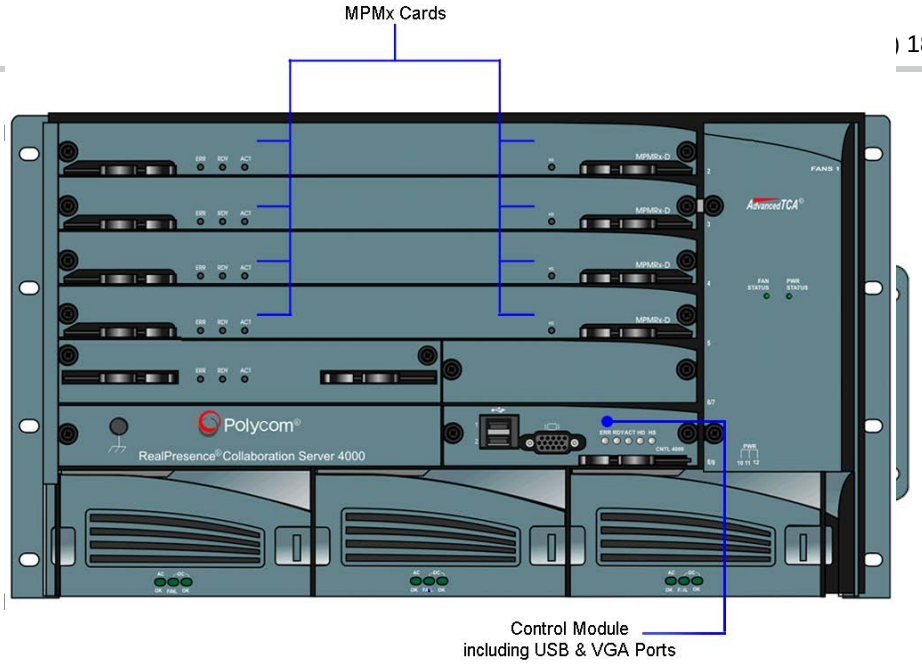
Please carefully review the following important upgrade notes:

- If your RMX system has MPMx cards, do not upgrade to RMX V8.6.7.
- Do not upgrade RMX 1500 systems to RMX V8.6.7, as they are not compatible with this release.
- It is essential you use the Backup Configuration function prior to upgrading your MCU. For more information see RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Administrator's Guide,
- It is essential you use the Backup Configuration function prior to upgrading your MCU. For more information see RealPresence Collaboration Server (RMX) 1500/1800/2000/4000 Administrator's Guide, Software Management.
- When upgrading it is recommended that you upgrade from the latest maintenance release of the version you currently have.
- Ensure that the Control Unit memory size is at least 1024MB. To check this, in the RMX Web Client or RMX Manager, go to Administration > System Information. If memory size is 512MB, DO NOT perform the upgrade procedure. Contact Polycom Support.
- If the upgrade process includes upgrading the Media cards, refer to the RealPresence Collaboration Server (RMX) 1800/2000/4000 MPMx Migration Procedure documentation.
- On Windows 7 systems, Protected Mode must be disabled before downloading the software. For information on how to do this, go to RMX Web Client System Requirements.

Collaboration Server (RMX) 2000/4000 Hardware / Software Compatibility

The Collaboration Server (RMX) 2000/4000 must be used with the correct software version:

- Collaboration Server (RMX) 2000/4000 systems shipped with MPMx media cards are not supported from software versions 8.6 and on.
- Both Control Modules BRD2534B-L0 / BRD2535B-L0 include USB and VGA ports on the front panel.


MPMx Cards
Polycom
RealPresence Collaboration Server 4000
Control Module
including USB & VGA Ports

Supported Upgrade Paths

The RealPresence® Collaboration Server includes a safety mechanism that ensures the installer chooses only a viable and safe software version for installation. It ensures that the current RMX software version and the new software installation are compatible and enables or rejects the software installation as required. When an incorrect or non-viable version upgrade/downgrade path is attempted, an alarm and fault are activated on the RMX. You can disable the safety upgrade mechanism by changing the default setting of the ENFORCE_SAFE_UPGRADE system flag to NO.
The following table lists the software versions that are approved for upgrade by Safe Upgrade process for Version 8.6.

Software Version	RMX 1800	RMX 2000	RMX 4000
8.5	Yes	Yes	Yes
8.4	Yes	Yes	Yes
8.3 (See note below)	Yes	Yes	Yes
8.2 (See note below)		Yes	Yes
8.1.8 (See note below)	Yes	No	No
8.1.5 (See note below)	Yes	No	No
8.1 (See note below)		Yes	Yes
7.8 (See note below)		Yes	Yes
7.7		Yes	Yes
7.6/7.6.1		Yes	Yes
7.5.0J/7.5.1J		Yes	Yes
7.2/7.2.x		Yes	Yes
7.1		Yes	Yes
7.0.x/7.0.2C		Yes	Yes
7.0		No	No
6.x		No	No
5.x		No	No
4.7.2		Yes	Yes

If your RMX version is not listed above, refer to the table below for intermediate and safe upgrade paths to Version 8.6.

Note: Upgrade from maintenance releases

When upgrading to version 8.6 from versions 7.8, 8.1, 8.2, and 8.3, it is essential that you upgrade from the following maintenance releases (or later) of the version currently installed:

- 7.8 - RMX_7.8.0.246.131
- 8.1.7 - RMX_8.1.7.37.033
- 8.2 - RMX_8.2.0.85.007
- 8.3 - RMX_8.3.0.148

If these maintenance releases (or later) are not installed, an upgrade to the latest maintenance release must be performed before upgrading to version 8.6. This is of particular importance for systems with 1024MB of memory.

Note: Upgrades from earlier versions

- When upgrading to version 8.6 from version 8.1 it is essential that you upgrade from the latest maintenance release of version 8.1 which is 8.1.7.37.033. If the latest maintenance release of version 8.1 is not installed, an upgrade to latest maintenance release of version 8.1 must be performed before upgrading to version 8.6. This is of particular importance for systems with 1024MB of memory.
- If you are upgrading from V7.0.1 or earlier please refer to the upgrade section of the version's release notes for more information about upgrading to V8.3 / V8.4.
- If your current version is 2.x, 3.x or 4.x, DO NOT upgrade to Version 8.6. Contact Polycom Support for the appropriate upgrade paths.

The following table lists the upgrade paths to Version 8.6.

Current Version	First Intermediate Upgrade		Second Intermediate Upgrade		Third Intermediate Upgrade		New Version	
	Version	Key	Version	Key	Version	Key	Version	Key
8.5	N/A		N/A		N/A		8.6	Yes
8.4	N/A		N/A		N/A		8.6	Yes
8.3	N/A		N/A		N/A		8.6	Yes
8.2	N/A		N/A		N/A		8.6	Yes
8.1	N/A		N/A		N/A		8.6	Yes
7.8	N/A		N/A		N/A		8.6	Yes
7.7	N/A		N/A		N/A		8.6	Yes
7.6/7.6.1	N/A		N/A		N/A		8.6	Yes
7.5.0J/7.5.1J	N/A		N/A		N/A		8.6	Yes
7.2 / 7.2.1 / 7.2.2	N/A		N/A		N/A		8.6	Yes
7.0.1 / 7.0.2 / 7.0.3 / 7.1	N/A		N/A		N/A		8.6	Yes
7.0	7.0.3	No	N/A		N/A		8.6	Yes
6.0.2	7.0.3	Yes	N/A		N/A		8.6	Yes
6.0 / 6.0.1	6.0.2	No	7.0.3	Yes	N/A		8.6	Yes
5.0.2	7.0.3	Yes	N/A		N/A		8.6	Yes
5.0 / 5.0.1	5.0.2	No	7.0.3	Yes	N/A		8.6	Yes

Upgrade Package Contents

The Version 8.6 upgrade package must be downloaded from the Polycom Resource Center and includes the following items:

- lan.cfg file
- LanConfigUtility.exe
- RealPresence Collaboration Server (RMX) 1800/2000/4000 Documentation
  - RealPresence Collaboration Server (RMX) 1800/2000/4000 Version 8.6 Release Notes
  - RealPresence Collaboration Server (RMX) 1800/2000/4000 Getting Started Guide
  - RealPresence Collaboration Server (RMX) 1800/2000/4000 Administrator's Guide
  - RealPresence Collaboration Server (RMX) 1800/2000/4000 Hardware Guide
  - Installation Quick Start Guide for RealPresence Collaboration Server (RMX) 1800/2000/4000
  - RMX Open Source Licenses
- External DB Tools
  - RealPresence Collaboration Server (RMX) 1800/2000/4000 External Database API Programmer's Guide
  - Sample Scripts
- RMX API Kit Version 8.6
  - RealPresence Collaboration Server API Version 8.6 Release Notes
  - RealPresence Collaboration Server XML API Overview
  - RealPresence Collaboration Server XML API Schema Reference Guide
  - MGC to RMX XML API Conferencing Comparison
  - Polycom XML Tracer User's Guide
  - XML Schemas
  - Polycom XML Tracer application
- Translations of RealPresence Collaboration Server (RMX) 1800/2000/4000,

  Getting Started Guide:
  - French, German, Japanese, Russian, Simplified Chinese, Hebrew and Portuguese

  Hardware Guide:
  - French, German, Japanese, Korean, Russian, Simplified Chinese, Spanish

To view the latest Polycom product documentation, visit the **DOCUMENTS & DOWNLOADS** section of the Polycom website at http://support.polycom.com.

Prepare for the Upgrade

To prepare for the upgrade:

1. If the Collaboration Server is used with a RealPresence DMA system, disable the RealPresence DMA system connection to the Collaboration Server:

a Log into the DMA system that handles call transfers for the Collaboration Server.

b Select Network > MCU > MCUs.

c Select the MCU and choose either Stop Using or Busy Out.

d Verify that all conferences, including permanent conferences, have been terminated.

2 If the MCU contains MPM or MPM+ cards:

a Make sure that these cards are disabled.

b Remove the MPM or MPM+ cards from the MCU and replace them with MPMRx cards.

c In the Hardware Monitor screen, click the reset button to reset the MCU.

3 Perform the upgrade as documented for your system.

Upgrading from Version 8.4 / 8.5 to Version 8.6

To upgrade to software version 8.6:

1 Download the Version 8.6.x.x.bin file from the Polycom Support Site.

2 On the RMX menu, click Administration > Software Management > Software Download.

3 Browse to the location where the Version 8.6.x.x.bin file was saved and click Install.

The **Install Software** information box indicates the file **Copying files is In progress**.

At the end of the Copying Files process, the system displays an indication that the software copying procedure is **Done**.

If the upgrade is not a supported upgrade path, the system will sound an alarm and an error message will appear.

When you acknowledge the error, the installation is aborted, and because the Safe Software Version Installation warning has been activated, your current browser session will block any new installation attempt. This applies to all software versions, except for version 7.6 which will still allow system downgrades.

When you have resolved the software compatibility issues, open a new browser session and attempt the installation again. If all issues have been resolved, the installation should complete.

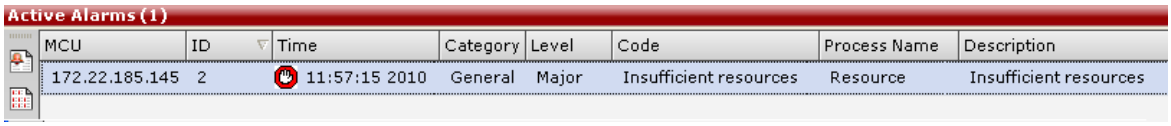
4 Click OK.

The upgrade procedure takes approximately 20 minutes. During this time:

- The **Install Software** information box indicates that Software Loading is in progress.
- A series of Active Alarms are displayed indicating the progress of the upgrade process.
- The **Install Software** information box indicates that IPMC Burning is in progress.

➢ A further series of Active Alarms are displayed indicating the progress of the upgrade process.

Sometimes, when updating the Version 8.6 license key, the system displays an active alarm shown below. Ignore this Active Alarm and complete this installation procedure.



5 If a message alert appears saying Please wait for system reboot, click Next.

Connection to the RMX is terminated and you are prompted to reopen the browser.

6 Close any open browser windows, wait approximately 10 minutes, and restart the browser.

7 Reconnect to the RMX by enter the IP address of the RMX Control Unit into the browser.

The version number in the **Welcome** screen has changed to 8.6.x.

8 In the **RMX Web Client – Welcome** screen, enter your **User Name** and **Password**, and click Login.

If the error “Browser environment error. Please close all the browser sessions” appears, close all the browser sessions, and reconnect to the RMX. If the error message appears again, either run the automatic troubleshooter utility or manually preform the suggested troubleshooting procedures.

In the Main Screen, an MCU State indicator displays a progress indicator 

showing the time remaining until the system start-up is complete.

To use the new features such as Operator Assistance and Gateway Sessions the IVR Services must be updated. For more details, see *Post Upgrade Configuration Procedures*.

9 As needed, reestablish the Collaboration Server connection to the RealPresence DMA system:

a Log into the DMA system that handles call transfers for the Collaboration Server.

b Select Network > MCU > MCUs.

c Select the MCU and choose Start Using.

d Verify that the version number is updated signifying that the upgrade is complete.

Post Upgrade Configuration Procedures

Upgrading the system can result in changes to default configurations system behaviors:

- **Permanent Conferences** must be manually re-scheduled.
- **IVR Services** should be checked after upgrading from earlier versions (V4.0 / V6.0 / V7.x / V7.6.1) to ensure that changed or additional DTMF codes do not conflict with previously defined DTMF codes.
- **Enable Gathering** check box in the **Profile Properties > Gathering Settings** tab is not selected by default for pre-existing Profiles.
- **SIP Proxy Registration** is configured in the **Conference Profile > Network Services** dialog beginning with version 7.1.

- **Media Encryption** is enabled by a Conference Profile setting from version V7.6.1, replacing the **ALLOW_NON_ENCRYPT_PARTY_IN_ENCRYPT_CONF** System Flag. Modified the profile to meet your environment's encryption requirements.
- **Automatic Muting of Noisy AVC-based Endpoints** is not automatically enabled in existing Profiles and has to be manually enabled, if required. In new Profiles that are created after the upgrade, auto mute of noisy endpoints option is enabled by default.
- **RealPresence DMA** in the environment requires that the value of the flag MAX_CONF_PASSWORD _REPEATED_CHAR System Flag value be set to 4 system for compatibility from version 7.7.
- **RMX Manager** for the specific version installed should be downloaded and installed. For more information see RMX Manager Application in the *RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Administrator Guide*.

Known Issues

The following table lists the known issues and suggested workarounds for this release of the RealPresence® Collaboration Server.

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-23835 / BRIDGE-24039	Audio	While in a conference call, audio bleeding was observed after approximately 2 hours and 18 minutes.	V8.6.3	Set ENABLE_SIR ENLPR to NO.
BRIDGE-19515	Audio	Audio Only calls from IBM Sametime fail to establish multipoint conference. Conference is created, but disconnection occurs after a few seconds.	V8.6	
BRIDGE-16334	Audio	The NoiseBlock feature is not functioning properly during audio cuts.	V8.5	
BRIDGE-24018	Audio	When connected to VMR RealPresence Collaboration Server (MPMRx), no audio from the Cisco TelePresence room is heard for the first 18 seconds.	V8.6.4	
BRIDGE-23490	Cascading	Sometimes, Lifesize Express 220 cannot dial into RealPresence Collaboration Server (MPMRx), which has been cascaded to RealPresence Collaboration Server, Virtual Edition.	V8.6.4	
BRIDGE-23519	Content	RealPresence Group Series dialing into a CP and SVC conference on RMX 1800 cannot send/receive content only when a Tandberg MXP already exists in the conference.	V8.6.4	
BRIDGE-24083 / BRIDGE-24060	Content	After RealPresence Collaboration Server (MPMRx) dialing out more than 100 Group Series and HDX participants and Group Series sharing content, participants get disconnected.	V8.6.4	
BRIDGE-6275	Content	When a Collaboration Server dials–out to a Viewstation endpoint, the Viewstation cannot receive content.	V8.1.6	
BRIDGE-18763 / BRIDGE-20053	Content	In a conference, H.323/SIP endpoints cannot snatch content token from ISDN endpoint currently sharing content, and vice versa.	V8.6	Stop sharing content by one endpoint before trying to share content by another endpoint.

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-13629	Content	On a call set to TIP Video & Content mode, some H.323 endpoints may not receive content.	V8.4	
BRIDGE-13192	Content	In a conference set to "TIP Video & Content" mode, Polycom ITP cannot send content.	V8.4	Use "Prefer TIP" mode.
BRIDGE-22710	Diagnostics	At times Web access to MCU is blocked due to antivirus policy.	V8.5.2	Log in though RMX Manager (though prevents Diagnostic mode).
BRIDGE-21599	Diagnostics	After a Logger Diagnostic File has been retrieved, and implementing the retrieving again, “Error in retrieving log file” message is reported.	V8.6.2	
BRIDGE-15596	Encryption	A dial-in SVC GS endpoint fails to receive video from the Collaboration Server in a Mixed encrypted conference. New endpoints joining the conference, cannot view the GS endpoint in their video as well.	V8.5	
BRIDGE-15263 / BRIDGE-16522	FECC	Failure to implement Far-End Camera Control between two Cisco endpoints connected (over H.323) to CP conference on Collaboration Server 1800.	V8.5	
BRIDGE-23845	General	The RealPresence Collaboration server continues to respond to infoRequest with callReferencevalue: 0 from DMA even though the system flag RESPOND_TO_H323_IRQ_CRV_0 value is set to NO. In some cases, the RealPresence Collaboration server experience high CPU utilization when large number of participants are connected to the system.	V8.5.4	
BRIDGE-23643	General	When sharing and snatching content from RealPresence Desktop endpoints, which are connected to a RMX 1800 with 90% ports are in use, " Internal communication Error" alarm displays and all calls are disconnected.	V8.6.4	
BRIDGE-9100	General	When using the Web Client, if a drop-down menu is selected and the user moves to another Internet Explorer Tab, the drop-down menu is displayed in the other tab.	V8.1.2	
BRIDGE-7454/ BRIDGE-9253	General	Site name displays (when it should not) on OTX and RPX endpoints when Telepresence Mode is set to Auto and ITP_CERTIFICATION flag is set to TRUE.	V8.2	

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-19510	General	Layout changes are delayed (3-4 seconds) in AVC 4M conferences on Collaboration Server 1800.	V8.6	
BRIDGE-18142	General	When an RMX 2000 is configured for “Separate Management Network” and is also configured to use 802.1X authentication on its IP Network Service interface, the status reported in the LAN List in the Hardware Monitoring pane may be inaccurate, showing the 802.1X Status as “Not Configured” and the 802.1X Method as “Off” even though 802.1X is configured.	V8.6	802.1X status can be determined by examining the status of the port at the 802.1X server.
BRIDGE-17718 / BRIDGE-20041	General	On Collaboration Server 1800, when Diffserv is selected as the QoS type, the documented default DSCP values are not actually used.	V8.6	
BRIDGE-15280	General	Collaboration Server 1800 crashes and reboots after a day-long conference.	V8.4 Inc 1	
BRIDGE-14559	General	Collaboration Server 1800 crushed and took 15 minutes to re-operate, following TCP dump via putty of media, during a conference with RPD endpoints sharing content. Log files did not reflect the reason.	V8.5	Run tcpdump via EMA to avoid memory crush due to using /tmp
BRIDGE-12768 / BRIDGE-17206 / BRIDGE-19745	General	In an SVC Mode conference, Group Series and RealPresence Desktop endpoints, dialing directly to an “Encrypt when Possible” VMR, are connected as Non-encrypted. When dialing via a Virtual Entry Queue they are erroneously connected as Encrypted. Occurs when SIP Transport type is TCP.	V8.4	
BRIDGE-10488	General	Audio and video in motion conference at 4Mbps on Collaboration Server (RMX) 1800 are more than five seconds out of sync on dial-in RealPresence Mobile and RealPresence Desktop endpoints.	V8.3	
BRIDGE-18420	Hardware	In RMX 2000 containing the new 1K power supply, following MPMRx media card reset, Collaboration Server cannot be turned on immediately following turn-off.	8.5.2	Wait at least 3 seconds between Turn-Off and Turn-On.

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-10139 / BRIDGE-16043 / BRIDGE-16736 / BRIDGE-16737	Hardware	New image installed on either the CF or SSD cards result in repeated system resets before reaching normal state.	V8.5	
BRIDGE-25362	Interoperability	Only in the Speaker Priority RMX conference, Cisco three-screen TelePresence systems display far site endpoint video on the left screen instead of center screen.	V8.6.7	
BRIDGE-25375	Interoperability	In the Prefer TIP VMR, Cisco TelePresence system cannot receive content from RealPresence Debut.	V8.6.7	
BRIDGE-24181	Interoperability	When Content Sharing is initiated from any endpoint in the VMR; the overall video stability of the call is affected and the transmitting video is lost from the system that initiates content. Endpoints also sometimes experienced permanent video freezing and loss of system functionality.	V8.6.7	
BRIDGE-24044	Interoperability	RealPresence Group Series and HDX cannot connect to a DMA VMR with settings of Secure when possible and Prefer TIP.	V8.6.4	
BRIDGE-23748	Interoperability	In the RealConnect call, the segment of speaker in the Cisco TelePresence Rooms does not display on Lync endpoint, instead the opposite segment displays.	V8.6.3	
BRIDGE-19517	Interoperability	LifeSize200 endpoint fails to display video and emits a loud buzzing in a CP 4M conference, when Collaboration Server 1800 dials out and connects over H.320 to said endpoint.	V8.6	
BRIDGE-18617	Interoperability	Cisco C20 and SX20 endpoints "connect with a problem" to an H.320 conference, based on the default conference profile, running on Collaboration Servers 4000 and 1800.	V8.6	
BRIDGE-18580 / BRIDGE-18777 / BRIDGE-19523 / BRIDGE-18580	Interoperability	In a combined Collaboration Server 4000 and CUCM (Cisco MCU) conference, CTS and TX TelePresence endpoints move from a Virtual Entry Queue (VEQ) to a Virtual Meeting Room (VMR), both on the DMA, fails - TX was disconnected, and CTS video froze.	V8.6	

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-15443	Interoperability	Following Collaboration Server failure, DMA failed to reestablish call on Collaboration Server 1800, when both Collaborations Servers were connected to the DMA from the call beginning.	V8.1.7, V8.5	Disable ICE.
BRIDGE-13638	Interoperability	Radvision Scopia XT5000 client not connected to RMX1800 MR in dial-out calls.	V8.4	Use dial-in
BRIDGE-13131 / BRIDGE-17196 / BRIDGE-19779	Interoperability	Polycom CX500 and CX600 IP phones disconnect after joining a call via dial out from a meeting room created on Collaboration Server (RMX) 1800.	V8.4	
BRIDGE-17408	ISDN	In a CP conference running on an RMX2000, the single ISDN endpoint is disconnected when many IP endpoints join the conference.	V8.6	
BRIDGE-18183 / BRIDGE-18420	MPM Card	MPMRx media card fails to come up following an RMX 2000, with 1KW power supply, reset by pressing Turn Off and On immediately.	V8.5.2	Wait at least 3 seconds between Turn Off and Turn On.
BRIDGE-16323 / BRIDGE-16746 / BRIDGE-16747/ BRIDGE-19998	MPM Card	A single media card supports up to 300 SVC participants in 60 conferences, with maximum 1.5 MB bit rate, such that each conference supports up to 5 participants.	V8.5	
BRIDGE-13130 / BRIDGE-17198	MPM Card	“Card voltage problem” alarm resulting from removal of MPMRx media card with Normal status from RMX 2000 is not cleared when the media card is reinserted.	V8.3, V8.3 Inc 1	Delete ISDN services before replacing the cards.
BRIDGE-20658	Partners - Microsoft	If the meeting organizer activates Mute Audience in a cascaded AVMCU conference, the AVMCU meeting organizer cannot de-activate Mute Audience by pressing Unmute Audience, resulting in the cascaded link to the RMX remaining muted.	V8.6	
BRIDGE-18779 / BRIDGE-20051	Partners - Microsoft	Connection cannot be established from an ISDN endpoint over a SIP gateway to a Lync client.	V8.6	

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-17887 / BRIDGE-20034	Partners - Microsoft	Collaboration Server sends an update to Lync Server every 10 minutes and the update fails.	V8.6	
BRIDGE-16637	Partners - Microsoft	Sometimes, no video received from Lync on iPad/iPhone when connected to a virtual meeting room on the Collaboration Server via a Lync Edge server.	V8.5	
BRIDGE-15747 / BRIDGE-16701 / BRIDGE-16729 / BRIDGE-20002	Partners - Microsoft	After disconnecting from an external Lync conference call, external Lync client users cannot reconnect to the call.	V8.5	
BRIDGE-15272	Partners - Microsoft	When both Polycom HDX systems and RealPresence Group Series systems registered to Lync attend a conference held on Polycom RealConnect using the content gateway, users might not be able to see shared content.	V8.5	
BRIDGE-13934 / BRIDGE-17174	Partners - Microsoft	Number of video Lync ICE participants is limited to 100. Beyond 100, participants will be connected as audio only participants.	V8.4	
BRIDGE-2347	Resource Capacity	When the system flag SEND_SIP_BUSY_UPONRESOURCE_THRESHOLD is enabled, and Port Gauge is 80% after many audio endpoints dial-in, a notification that the audio threshold has been exceeded is not sent.	V8.0	
BRIDGE-19513	Resource Capacity	Extra 2 ports (12 instead of only 10) are declared available, though using them results in poor performance, in Collaboration Server 1800 with no DSP cards.	V8.6	
BRIDGE-17352	Resource Capacity	In a Video Switching Conference on Collaboration Server (RMX) 1800, each video endpoint consumes one HD port irrespective of the Conference Line Rate.	V8.5	
BRIDGE-13788	Resource Capacity	Failure to connect more than 193 HD AVC endpoints in a conference dialing in to two Virtual Meeting Rooms via DMA.	V8.4	

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-18570	RMX Web Client	Some customers may experience difficulties in using the RMX Web Client to access the Collaboration Server's management console as a result of local IT policy or the actions of certain Anti-virus applications on the control workstation.	V8.5.2	Use the Local Web Client (RMX Manager) application by: Installing from RMX Web Client Login page -or- downloading and installing fromthe Polycom Support site.
BRIDGE-20232	Security	At times, when either modifying DNS address from IPv4 to IPv6, or modifying shelf management IPv6 address, Collaboration Servers with MPMRx media card failed to restart either completely or in a timely manner. Also, POLYCOM administrator user was locked, and only SUPPORT administrator user can be used.	V8.6	
BRIDGE-20202	Security	When launching a conference from a GS endpoint registered as AS-SIP, on a Collaboration Server 1800 using IPv4 address mode, the endpoint IP address cannot be viewed via **Participant Properties > Channel Status - Advanced** tab.	V8.6	
BRIDGE-17625	Security	Reboot required following new CRL installation on Collaboration Server 2000, for new CRL to take effect.	V8.6	Reboot RMX periodically to ensure that the latest CRLs take effect.
BRIDGE-9814	SIP	A RealPresence Mobile client running on iOS connecting using SIP to an AVC only conference with the content profile set to H264 Cascade and SVC Optimized cannot receive content.	V8.3	
BRIDGE-17269	SIP	A RealPresence Mobile client running on iOS connecting using SIP to an AVC only conference with the content profile set to H264 Cascade and SVC Optimized cannot receive content.	V8.3	

Known Issues

Issue ID	Category	Description	Found in Release	Workaround
BRIDGE-18707 / BRIDGE-19516	Software Version	Following upgrade from 8.5 to 8.6 of Collaboration Server 4000 with MPMRx media cards, and license activation, an “MPL failure - product activation indication was not received”, MCU state is indicated as MAJOR, available ports cannot be viewed, and at times no connection with the switch appears.	V8.6	
BRIDGE-17224	Software Version	On Collaboration Server (RMX) 1800, DTMF Codes (Enable Roll Call, Disable Roll Call, Roll Call Review Names, Roll Call Stop Review Names, Invite Participant, Disconnect Invited Participant, Override Mute All) are missing from DTMF Codes dialog following upgrade from 8.1 to 8.4.	V8.1.8	
BRIDGE-14125	Upgrade Process	During upgrades from RMX v8.3 to v8.4, users may receive a “no connection with switch” error when trying to access the hardware monitor via EMA\RMX manager. The system functions normally.	V8.4, V8.5	Soft reset clears error condition.
BRIDGE-23853	Video	Sometimes, flickering video displays on SVC GroupSeries endpoints.	V8.6.4	
BRIDGE-9369	Video	In a 4096 kbps conference with site names and message overlay enabled whose Video Quality is set to Motion, the next on an HDX using 4CIF resolution saw stretched text while endpoints using other resolutions received correctly proportioned text.	V8.1.5	
BRIDGE-17276	Video	In a 4096 kbps conference with site names and message overlay enabled whose Video Quality is set to Motion, the next on an HDX using 4CIF resolution saw stretched text while endpoints using other resolutions received correctly proportioned text.	V8.1.5	
BRIDGE-17266	Video	VSX receives no video in SIP call registered to DMA.	V8.3	
BRIDGE-13890	Video	When TIP compatibility is set to "Video & Content" RP Immersive Studio does not receive video on its primary (center) screen.	V8.4	Use "Prefer TIP" mode.
BRDIGE-19509	Video	MXP endpoint is “Connected with problem” and fails to send video, when connected to a conference on Collaboration Server 1800 over H.320.	V8.5	
BRIDGE-23369	Video	When selecting “View Participant Sent Video” or “View Participant Received Video” in RMX Manager on the workstation with AMD GPU, the black video instead of previewed video displays.	V8.3	

Resolved Issues

The following sections list the issues that have been resolved in the RealPresence® Collaboration Server version 8.6 branch of software.

Issues Resolved in This Release

The following table lists the issues resolved in this release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-25540	Audio	In the Prefer TIP RealPresence DMA VMR (RMX 1800), no audio is heard from TIP-enabled RealPresence Group Series that is registered in RealPresence DMA.
BRIDGE-25527	General	Major alarm of detecting new core files raises and all endpoints are disconnected from RealPresence Collaboration Server (MPMRx).
BRIDGE-25520	Interoperability	In the Prefer TIP conference on RealPresence Collaboration Server (MPMRx), single screen endpoints are not seen as Active Speaker on other single screen systems.
BRIDGE-25512	Interoperability	Cisco TelePresence IX5000 left and right screens are not shown in the Prefer TIP conference.
BRIDGE-25303	Interoperability	In a RealConnect conference with DMA VMR, RMX rejects non-encrypted endpoints even though encryption set to whenever available.
BRIDGE-25009	Interoperability	Calls failover from RMX 2000 to RMX 1800 fail and the calls are indicated as duplicated conferences when connecting to RMX 1800.
BRIDGE-24909	FECC	Far End Camera Control (FECC) does not work as expected. A first command is ignored by the system, a second comment causes both commands to be issued.
BRIDGE-24870	IVR	After upgrading to version 8.6.4.97, IVR welcome slides no longer work in Entry Queue.
BRIDGE-24860	RMX Manager	A system reset from RMX Manager fails on RMX 1800.
BRIDGE-24782	Cascading	In the RealConnect conference, standards-based endpoints on the RMX are able to see all endpoints, but Skype for Business endpoints are not able to see standards-based endpoints.
BRIDGE-24764	Gateway	While in VEQ, a Segmentation Fault in ConfParty process occurs and core dump is created.
BRIDGE-24712	Security	After ENABLE_TLS_V_1_0 is set to YES, RealPresence Collaboration Server fails in fallback to align with the TLS1.0 setting on RealPresence DMA, thus calls are not connected.
BRIDGE-24681	Reservations	Adjusting the end time of a schedule does not lead to the recalculation of the schedule duration.

Issue ID	Category	Description
BRIDGE-24663	MPM Card	RMX2000 with MPMx-D cards stops accepting new calls until the system was rebooted.
BRIDGE-24631	General	During Lync direct call with various endpoints with load more than 40%, MIPS along with MFA Error faults are generated.
BRIDGE-24557	Interoperability	In DMA system VMR conferences, several endpoints are disconnected from the conference at the same time.
BRIDGE-24502	SIP	On RMX, the SIP endpoint gets disconnected from a VMR conference.
BRIDGE-24468	SIP	In a RMX 1800 conference call, the openSSL stack throws an error when the siptask tries to send a reINVITE over TLS.
BRIDGE-24329	IVR	While moving from a Virtual Entry Queue (VEQ) to a Virtual Meeting Room (VMR), the endpoint receives an invalid conference ID IVR message after dialing the correct conference ID.
BRIDGE-24313	Interoperability	In a DMA system VMR conference, Skype for Business clients are dropped from VMR and reconnection attempts result in busy tone and no connection.
BRIDGE-24257	General	In the RMX system Address Book, when participant is moved to a different group using drag and drop, the mouse cursor tooltip shows the icon for a copy operation.
BRIDGE-24244	IVR	While moving from a Virtual Entry Queue (VEQ) to a Virtual Meeting Room (VMR), the endpoint receives an invalid conference ID IVR message after dialing the correct conference ID.
BRIDGE-24241	Interoperability	While RMX 4000 system crashed and rebooted, all ongoing conferences were forcibly disconnected.
BRIDGE-24210	Video	When a third-party endpoint joins an RMX system conference (dialed via SIP through a DMA system) using the TIP protocol, the endpoint will get incorrect video layouts.
BRIDGE-24071	General	A new core file was detected--SystemMonitoringNew:ConfParty causing an RMX system reboot.
BRIDGE-24059	General	User received a Web UI alert of ‘ailed to Preview Video: Failure Status. The maximum number of previews per MCU has been reached" when attempting to preview video from an RMX participant.
BRIDGE-24049	Audio	When an audio (POTS) participant is added to an H.323 call that is occurring on the MCU at 720p or 1080p, the call then downgrades to SIF.
BRIDGE-24045	Interoperability	After holding and resuming the 384/512/768 Kbps call on RMX 1800, RealPresence Group Series 310 is connected in 64 Kbps resulting in layout does not show in video on near and far ends.
BRIDGE-24021	Interoperability	On a Cisco DX endpoint, BFCP content doesnot work with the RMX system.
BRIDGE-23961	General	New core file was detected as httpd received an abort signal and crashed the system.

Issue ID	Category	Description
BRIDGE-23924	Partners - Microsoft	In a VMR call, all Polycom ContentConnect plug-in clients get disconnected and are not able to rejoin. Their respective Lync clients connect normally.
BRIDGE-23881	MPM Card	Error indicating no link is between FSW 4000 and MPMRx card in slot 2 displays followed by the card reboot.
BRIDGE-23548	MPM Card	MPMRx card reset occurs after MFA core dump is generated.

Issues Resolved in Version 8.6.4

The following table lists the issues resolved in the 8.6.4 release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-23491	Audio	When connecting Group Series 500 to RealPresence Collaboration Server (MPMRX), lip-sync error and audio clipping occur. Setting ENABLE_SELECTIVE_MIXING to Yes causes audio clipping in some cases.
BRIDGE-22258	Audio	When following re-invite, the audio codec is modified by the Collaboration Server, endpoints do not receive the audio.
BRIDGE-22534	Audio	Random participant can be heard by some participants but not heard by others in the same VMR.
BRIDGE-22482	Cascading	In an audio-only cascading conference, RAPD participant needs to be set to Slave to make audio flow is bidirectional; otherwise the audio flow will be unidirectional to the default Master (automatically set).
BRIDGE-22637	Cascading	In a cascaded conference, sharing content consumes excessive bandwidth then line rate configured in conference profile.
BRIDGE-22435	Content	Content sharing drops between remaining endpoints after RealPresence Mobile user disconnects from meeting.
BRIDGE-23826	Content	When using RMX web client, the user cannot view the content shared in the conference.
BRIDGE-23460	Content	When a WebSuite participant shares and stops content, all other participants see frozen content on their screens.
BRIDGE-23464	Content	ContentConnect content quality is toggling between low resolution and high resolution during the same RealConnect conference.
BRIDGE-22477	Content	RMX(Rx) cannot share 1080p content when Group Series endpoints with/without 1080p option in the same conference.
BRIDGE-22916	Content	In a cascading link, when a lecture is set to “Change To Content Token Owner”, other participant can still share content.
BRIDGE-21963	Content	Video Quality deteriorates after sharing Content when using RMX with MPMx media cards.
BRIDGE-22942	Content	In a conference with 1920 kbps line rate, content shared from Sony PCS-XG100 is not displayed on both near-end and far-end.
BRIDGE-23192	Content	After moving a Lync and CSS client from a conference with password to another conference without password, while a Group Series endpoint is sharing the content in the latter conference, the Lync and CSS client cannot receive the content until the Group Series restart the content.
BRIDGE-23248	Diagnostics	When logging in RealPresence Collaboration Server (MPMRx) with password “&aaaa9999%aaa9999#”, Hardware Monitor displays abnormal.

BRIDGE-22489	Encryption	Call from HDX via Acme SBC to DMA VMR using “Encrypt When Possible” setting fails with call rejected by RMX.
BRIDGE-22919	Gateway	Gateway call from SIP endpoint to ISDN-Video endpoint fails.
BRIDGE-22714	Gateway	When both audio and video participants indications are enabled on Collaboration Server, video participants joining from another Gateway in the VMR are not counted and shown on other participant’s screen. Audio Gateway participants are counted correctly.
BRIDGE-23100	General	During a long conference call in RMX 1800, a core dump gets created.
BRIDGE-23414	General	After a conference profile is created without telepresence selected, and a participant’s layout is changed from conference layout to personal layout, RealPresence Collaboration Server (MPMRx) prompts error: “Failed to delete participant: Personal layout is managed internally in telepresence mode.”
BRIDGE-22690	General	Alarm “Failed to register with OCS. Check the RMX Server Name.” displays in Fault List, and then is cleared automatically. The alarm displays about every hour.
BRIDGE-23079	General	RealPresence Collaboration Server (MPMRx) undergoes unexpected restart.
BRIDGE-22908	General	Importing address book from one RealPresence Collaboration Server to another will result in various groups no longer present in the address book.
BRIDGE-22758	General	Unable to change personal layout in participant’s properties dialog.
BRIDGE-23066	General	After configuring TCP Fixed Ports on IP Network Service of RMX 4000, RMX 4000 fails to update the configuration and "Invalid TCP Ports" alarm is generated.
BRIDGE-22486	General	Collaboration Server drops all calls, and “8751ConfPartyMedia is recovering” displays in Fault List.
BRIDGE-22726	General	Endpoints cannot disconnect from DMA VMR, the endpoints are stuck in disconnecting state, and the conference cannot be deleted.
BRIDGE-22481	General	RMX using MPMx media cards rebooted with message "Internal MCU resetMcmsDaemonMcmsDaemon reset due to WD policy decision: Process failed [0:0] : ConfParty".
BRIDGE-22483	General	Core dumps seen in Faults List on RMX using MPMx media cards.
BRIDGE-22487	General	When initiating access to Shelf Management IP via Web browser, the login page is blank, and the login fails.
BRIDGE-22716	General	RMX is no longer able to display Address Book from Resource Manager using port 443 after upgrading Resource Manager from v8.2.1 to v8.4.1, on RMX Appliance and Virtual Edition MCUs.
BRIDGE-22492	General	ICE doesnot function if DNS is not configured in Management Network Service on RealPresence Collaboration Server.
BRIDGE-22493	General	When IP Network service is configured to Microsoft, RMX is unable to receive DTMF in calls to the Virtual Entry Queue.

BRIDGE-22629	General	RMX (Rx) system becomes unresponsive, then followed with a reboot. After the reboot, RMX becomes operational as normal.
BRIDGE-22523	General	Duration does not display correctly as configured for Meeting Room.
BRIDGE-22546	General	H.264 high profile check box is not shown on General tab of Conference profiles when creating the New Conference Profile.
BRIDGE-22623	General	After the conference ID being deleted and meeting room being saved, “Internal communication error” displays followed with RMX 1800 restarts.
BRIDGE-22925	General	After RealPresence Collaboration Server dialing out to an endpoint and the endpoint user selecting “ignore incoming call” manually, the RealPresence Collaboration Server still attempts to redial endpoint.
BRIDGE-23244	General	After a RMX 1800 without DSP card being upgraded from v8.5.1.16 to v8.6.3.29, the system shows itself with three DSP cards incorrectly.
BRIDGE-23023	General	"Registration failed for some Conference" alarm shows every 15 minutes on RMX 1800.
BRIDGE-23536	General	When changing the display name of meeting room, the change does not show in properties of the meeting room and participants of the meeting room.
BRIDGE-22479	H.323	Core Dump generated when RMX using 2 MPMX cards crashed during conference.
BRIDGE-23756	Hardware	RealPresence Collaboration Server undergoes unit failure and gets disconnected from socket. This is followed by a card reboot.
BRIDGE-23709	Hardware	RMX 4000 core dump files are created and RMX 4000 reboots.
BRIDGE-23740	Interoperability	Hung calls experienced from MGC cascade, and participant or conference with a participant cannot be deleted when using RMX with MPMRx media cards.
BRIDGE-21363	Interoperability	RPX or TPX ITP room containing HDXs as the last participant isn't automatically terminated from the conference on RMX 2000 when using RMX with MPMx or MPMRx media cards.
BRIDGE-23310	Interoperability	When an OTX call is connected to the RealPresence Collaboration Server (MPMRx), which is in Speaker Priority mode, the active speaker’s one-camera room view displays in each of the three screens.
BRIDGE-23277	Interoperability	Call from HDX via ACME SBC to DMA VMR with encryption set to whenever available fails because the call is rejected by the RealPresence Collaboration Server.
BRIDGE-23153	Interoperability	RealPresence Collaboration Server loses connection with RealPresence DMA, all calls drop.
BRIDGE-22484	Interoperability	Hung calls experienced from MGC cascade, and participant or conference with a participant cannot be deleted when using RMX with MPMRx media cards.

BRIDGE-22361	Interoperability	Call bitrate setting in Conference Profile on a RMX Virtual Edition MCU does not correctly limit the call connection bitrate in calls from a HDX endpoint.
BRIDGE-22502/ BRIDGE-22510	Interoperability	When using Collaboration Server (MPMRx), all participants lose audio in DMA VMR.
BRIDGE-22485	Interoperability	After a RealPresence Collaboration Server is configured with 384kbps and AES encryption, and dialing out to an HDX being connected with Siren22, packet loss occurs constantly in the transmit direction from HDX to RMX.
BRIDGE-23226	Interoperability	Call speed and resolution mismatch between RealPresence Desktop and VSW high profile of RealPresence Collaboration Server.
BRIDGE-22480	IP	Creating the second IP Network Service through either RMX Manager or Web client on RMX 1800 fails, “Failed to add IP Network Service: Maximum number of Service already defined” message is reported.
BRIDGE-23618	ISDN	RMX 2000 cannot receive ISDN-Video calls but can receive ISDN-Voice calls.
BRIDGE-22780	IVR	IVR plays invalid password message to un-registered SIP participants. Also occurs when the password is contained within the dial string.
BRIDGE-22544	IVR	Participants’ endpoints do not forward the "Invite Participant” DTMF code in ISDN calls on RMX Appliance and Virtual MCUs.
BRIDGE-22494	IVR	Cannot delete participant from the Entry Queue when using RMX (Rx).
BRIDGE-22752	IVR	At times, mobile phone participant cannot hear IVR message for typing conference passcode.
BRIDGE-23533	MPM Card	MPMRx card powers off with MFA core dump.
BRIDGE-23160	MPM Card	Participants cannot hear each other in a call lands on MPM card 2 fails.
BRIDGE-22490	MPM Card	An MPMRx card crash, likely resulting from audio/video UDP ports indicated by the logs as not released following conference end.
BRIDGE-23105	Multilingual	In the RealConnect conference, if the Site Name of Lync participant includes Latin ISO character, that is “é”, the character displays as “?”.
BRIDGE-23523	Partners - Microsoft	When the Lync 2013 client with CSS plugin connecting to the RealPresence Collaboration Server VMR, the client cannot see the message overlay.
BRIDGE-23603	Partners - Microsoft	VMR Lync calls are disconnected due to ICE check failure.
BRIDGE-23380	Partners - Microsoft	If a RealConnect conference including both of Skype for Business participant and RealPresence Desktop participant, RealPresence Collaboration Server participants receive frozen video.
BRIDGE-22848	Partners - Microsoft	When using RealConnect, Trio endpoint connected to the AVMCU receives no video or low resolution video on RealPresence Collaboration Server.
BRIDGE-22035/ BRIDGE-22044	Partners - Microsoft	ContentConnect failed to resume following network failure, in a meet-now (ad-hoc) conference initiated by a Lync client, and using a Virtual Meeting Room (VMR) to connect to non-Lync clients.

BRIDGE-22261	Partners - Microsoft	Collaboration Server RealConnect cascaded link remains muted, though Presenter of Lync conference unmuted the audience.
BRIDGE-22488	Partners - Microsoft	During a RealConnect conference, Lync participants cannot view non-Lync video participants.
BRIDGE-22650	Partners - Microsoft	When a Room System joins a RealConnect call initially having had 2 LifeSize Room Systems connected via Lync AVMCU, from which 1 of the initial LifeSize Room Systems has disconnected, twitching pvideo is experienced when using RMX Virtual Edition MCU.
BRIDGE-23098	Partners - Microsoft	RealConnect participants/CSS GW is disconnected from RealPresence Collaboration Server (MPMRx).
BRIDGE-23555	Recording	Start recording a RealConnect conference by the HDX remote control fails.
BRIDGE-22491	Recording	Recording does not start after clicking “Start Recording” on RMX Web UI, instead the recording starts after clicking “Stop Recording”.
BRIDGE-23553	Reservation	Conflict conferences can be wrongly reserved, although the conference will not be launched.
BRIDGE-22655	Reservation	Reservation conference changes to suspended after system reboot.
BRIDGE-22801	Reservation	When creating a reservation or changing other configurations of a reservation, the duration value changes itself.
BRIDGE-22501	Resource Capacity	Audio calls transferred from a VEQ to a Mixed-Mode VMR consume video resources instead of audio resources in conference on RMX using MPMx, MPMx, MPM+ media cards.
BRIDGE-22985	Security	After the Secured Communication is enabled, RealPresence Collaboration Server fails to save the entered H.323 authentication user name and password. The user name and password fields are still empty after reboot.
BRIDGE-24040	Video	While endpoints are connected to the DMA VMR, Lync 2010 clients face the issue of low resolution video and video freeze.
BRIDGE-22896	Video	RMX 1800 with 1920 kbps Motion conference profile configured does not send video in correct frame rate, that is 60fps.
BRIDGE-22753	Video	When 512Kbps and “Video Quality Optimized” is configured, call from Collaboration Server to GS300 connects at 720p first but soon changes to 4CIF.
BRIDGE-22748	Video	In a multi-point call, some codecs show a pink stripe on the far end video.

Issues Resolved in Version 8.6.3.6_1186

The following table lists the issues resolved in the 8.6.3.6_1186 release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-21679	Upgrade Process	Upgrade to 8.6.3.6 fails due to RTM IP card endless upgrade. V8.6.3 Note: A new *RMX _8.6.3.6_1186.bin* is developed to replace the *RMX _8.6.3.6.bin*.

Issues Resolved in Version 8.6.2

The following table lists the issues resolved in the 8.6.2 release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-20369	Interoperability	When using Collaboration Server (MPMRx), all participants lose audio in DMA VMR.

Issues Resolved in Version 8.6.1

The following table lists the issues resolved in the 8.6.1 release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-20367/ BRIDGE-20372/ BRIDGE-20515	Audio	In some conferences on Collaboration Server with MPMRx system, participants cannot hear audio but they can see the video, some of the participants are disconnected from the conference.
BRIDGE-20650	Audio	PSTN participant who dials into conference on RMX 1800 cannot hear other ISDN and H.323 voice participants, but the PSTN participant can be heard by other voice participants.
BRIDGE-19169	Cascading	In cascading environment, conference on Master Collaboration Server cannot be deleted.
BRIDGE-20447	Cascading	When a RealConnect call is established between Collaboration Server and AVMCU, and the content is sent by one RMX participant, the participant has duplicated video displays, one is the real participant video in the RealConnect conference, the other is the default Lync blue silhouette for CSS.
BRIDGE-19239	General	Media Traffic Shaping malfunctions every third time in Collaboration Server MPMRx system reaches 160 Kbits per 0/1 seconds.
BRIDGE-19296	General	Call flow timing issue causes call drops in the active conference on Collaboration Server.
BRIDGE-19438	General	After upgrade and restore the backup on Collaboration Server, Address Book is not accessible and becomes empty.
BRIDGE-19492	General	After frequent layout changes in the Video Setting of Conference Properties window, and Conference Properties window is kept open, RMX manager response becomes slow.
BRIDGE-19552	General	Collaboration Server with MPMRx system reboots due to internal Collaboration Server reset and core dump.
BRIDGE-20010	General	Collaboration Server with MPMRx system drops calls and reboots, and high CPU utilization is reported in Fault List.
BRIDGE-20146	General	SIP participants are abruptly disconnected from ongoing conference on Collaboration Server with MPMRx system due to video transmit rate decrease.
BRIDGE-20267	General	ISDN participants cannot be added or removed on Collaboration Server with MPMRx system after a core dump.
BRIDGE-20334	General	Some conferences remain active and cannot be removed from Collaboration Server with MPMRx system after the call has ended.
BRIDGE-20396	General	PARTY_IDENT_INFO is added in Visual Name.
BRIDGE-20451	General	After Message Overlay is disabled in a conference on Collaboration Server with MPMRx system, and an endpoint is disconnected and reconnected, the Message Overlay displays again on the screen of the endpoint.

Issue ID	Category	Description
BRIDGE-20509	General	Uncommanded reboot of Collaboration Server with MPMRx system causes calls drop.
BRIDGE-20569	General	ICE stack and CNTL process error causes Collaboration Server with MPMRx system crash, video calls drop and cannot reconnect.
BRIDGE-20581	General	Collaboration Server with MPMRx system spontaneously disconnects audio and video participants.
BRIDGE-20627	General	Collaboration Server with MPMRx system experiences slowness in the GUI, followed by MCCF disconnects messages, high CPU utilization, and eventually a ConfParty Crash and MCU reset.
BRIDGE-19141	Hardware	Even though LAN port of RTM IP card is in connection, Port Speed of ShMG (Shelf management) port on Collaboration Server with MPMRx system is reported incorrectly, which is reported as 10 Half Duplex.
BRIDGE-19571	Hardware	Collaboration Server with MPMRx system automatically restarts due to temperature issue of CNTL module.
BRIDGE-20150	Interoperability	In a RealConnect environment, call connection fails from DMA to Collaboration Server with MPMRx system.
BRIDGE-20166	Interoperability	MCCF error is reported on Collaboration Server in the process of DMAs Failover and primary DMA service recovery.
BRIDGE-20384	Interoperability	Video issues and Audio issues exist in some ATX-300 rooms, when more than 18 rooms are connected to RPRM pooled conference hosted by Collaboration Server with MPMRx system. Only the 1080p calls are affected. When more than 54 endpoints connected, every call is affected.
BRIDGE-20521	Interoperability	When highest CP resolution is set to 720p30 on Collaboration Server and the maximum bit rates of HD 720p30 resolution is set to 512kbps in the Sharpness mode-High Profile resolution slider, endpoints HDX4500 and HDX 8000 with 1024K set in their profile cannot receive video from Collaboration Server.
BRIDGE-20530	Interoperability	In the call from CTS 3000 to Collaboration Server when participant's location is between two microphones, duplicated audios from the same participant are generated. The sound effect is echo-like.
BRIDGE-20612	Interoperability	When the Line rate configuration on Collaboration Server with MPMRx system media card is higher than the Max Per-Call bandwidth configuration on DMA, the SIP calls to RMX are rejected by the DMA due to the RMX requests higher bandwidth.
BRIDGE-20303	MPM Card	MPMRx media card undergoes FPGA recovery after DSPs stop responding to keepalive.
BRIDGE-20308	MPM Card	When installing MPMRx media card, packet loss occurs. The video freezes and the audio is choppy. MPMRx card isn't shown under Ethernets Settings or LANs as expected.
BRIDGE-19406	MPM Card	MPMRx media card on Collaboration Sever with MPMRx system crashes due to DSP issues.

Issue ID	Category	Description
BRIDGE-19474	Partners - Microsoft	Lync VM snapshot operation causes Collaboration Server with MPMRx system loose registration in Lync 2013 FE server, then Collaboration Server stops processing inbound and outbound Lync calls and produces core dump.
BRIDGE-20633	Partners - Microsoft	In a RealConnect environment, Collaboration Server with MPMRx system is registered with Lync FE pool, and load balancing is through a hardware load balancer. After rebooting the Collaboration Server, the SIP registration is successful, but the Lync Edge server registration fails.
BRIDGE-20593	Resource Capacity	Collaboration Server with MPMRx system has insufficient resources for max capacity stated in the license, Collaboration Server disconnects from DMA.
BRIDGE-19357	Video	After Collaboration Server with MPMRx system is upgraded, and the Telepresence Mode is set to On, personal Layout in Participant Properties becomes not configurable.
BRIDGE-20597	Video	When a participant disconnects from a conference on Collaboration Server, upon reconnecting, the participant's framing goes back to the default conference level framing, 1x1 Auto.

Issues Resolved in Version 8.6

The following table lists the issues resolved in the 8.6 release of the RealPresence® Collaboration Server.

Issue ID	Category	Description
BRIDGE-16723	Audio	Unsynchronized audio and video in CP and Mixed CP and AVC conferences on Collaboration Server with MPMRx media card.
BRIDGE-19443 / 19520	General	Green and purple artifacts on AVC endpoints' layout following a speaker change from SVC to AVC, in a 2M mixed conference with 80% load (whether line rate or configurations), and 5 SIP SVC plus 11 H.323 AVC endpoints connects.
BRIDGE-18441	General	The system is exposed to attacks running arbitrary code using current user permissions, due to a bug in one of the standard libraries used for code development.
BRIDGE-17351	General	SIP registration fails in an RMX conference running in ultra-secure mode in auto configuration for IPv6 with OCSP on, and the IPv6 global responder URL specified.
BRIDGE-16753	Interoperability	On RMX1800 single screen Cisco TelePresence systems cannot send content in Prefer TIP Conference.
BRIDGE-16466 / 16730	Interoperability	During a conference held on Collaboration Server using Multipoint Layout Application (MLA) and Polycom RealConnect technology, an AVMCU might show a layout and not the active speaker when TelePresence endpoints are in the call.
BRIDGE-16414	Interoperability	When using MPMRx media cards, Polycom VVX600 endpoint registered to CUCM connects with 'Connected With Problem' status to RMX conference with 'Prefer TIP' selected in the Profile. VVX600 endpoint registered with DMA connects successfully.
BRIDGE-14466 / 15673 / 16778	ISDN	When replacing RTM-ISDN-12-ports card with RTM-ISDN-9-PRI-ports card (and vice versa), the number of PRI ports is not updated to match the new card.
BRIDGE-13376	IVR	On Collaboration Server (RMX) 1800, DTMF Codes (Enable Roll Call, Disable Roll Call, Roll Call Review Names, Roll Call Stop Review Names, Invite Participant, Disconnect Invited Participant, Override Mute All) are not listed in DTMF Codes dialog after upgrading MCU from 8.1.8.98 to 8.4.0.298.
BRIDGE-11461 / 16853	Multilingual	When the alert, "SSH is enabled" was translated into Chinese, the Chinese equivalent was "Music file failed".
BRIDGE-16693 / 16694	Partners - Microsoft	When both Polycom HDX systems and RealPresence Group Series systems registered to Lync attend a conference held on Polycom RealConnect using the content gateway, users might not be able to see shared content.
BRIDGE-16418	Partners - Microsoft	During a conference hosted by Collaboration Server 1800, VVX business media phones disconnect from the conference after a held call is resumed on the VVX.

Issue ID	Category	Description
BRIDGE-12479/ 14058	Partners - Microsoft	On MPMRx systems cascaded to Lync 2013 AVMCU, video freeze may occur on some endpoints connected to RMX if Lync 2010 and Lync 2013 clients connect to the AVMCU simultaneously. Video resumes after a short period. In most cases this scenario will result in single DSP failure and there will be swap of the media to another DSP, which mean short video freeze to the user. There could be instances in which the freeze would be longer than few seconds, as the sequence of swaps should end and it takes several seconds for each swap to be completed.
BRIDGE-17353/ 17354	Resource Capacity	In a Video Switching Conference on Collaboration Server 1800, each video endpoint consumes one HD port irrespective of the Conference Line Rate.
BRIDGE- 17521 / 17621 / 17622	Video	Abnormal video, specifically, the cut edges on left and right sides and the black borders at top and bottom, when dialing from a VVX endpoint into a CP conference running on Collaboration Server 1800 with no DSP cards, at 1920Kbps.

Get Help

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

To find all Polycom partner solutions, see Polycom Global Strategic Partner Solutions.

The Polycom Community

The Polycom Community gives you access to the latest developer and support information. Participate in discussion forums to share ideas and solve problems with your colleagues. To register with the Polycom Community, create a Polycom online account. When logged in, you can access Polycom support personnel and participate in developer and support forums to find the latest information on hardware, software, and partner solutions topics.

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 integrations. For additional information and details please see http://www.polycom.com/services/professional_services/index.html or contact your local Polycom representative.

Copyright and Trademark Information

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom 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 property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

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.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.

NEW FEATURE DESCRIPTIONS

Polycom® RealPresence® Collaboration Server (RMX®) 1800/2000/4000

This document describes the new and changed features of the RealPresence® Collaboration Server version 8.6 releases.

Contents

Version 8.6.7 Detailed Description of Changed Feature

Version 8.6.4 Detailed Description of Changed Feature

Version 8.6.2 Detailed Description of New Features

Version 8.6 Detailed Description of New Features

Version 8.6.7 Detailed Description of Changed Feature

TLS 1.1 and TLS 1.2

In addition to TLS 1.0, in this release APACHE, Central singling, LDAP, EXCHANGE and ICE (TURN) are able to communicate on TLS1.1 and TLS 1.2.

Following table show the TLS version supported on different feature:

TLS Version Support by Functions

Function	TLS Version
APACHE	TLS 1.0, TLS 1.1, TLS 1.2
Central singling and LADP	TLS 1.0, TLS 1.2
EXCHANGE	TLS 1.2
ICE	TLS 1.2

System Flags for Changing TLS Version

Followings are system flags for setting TLS versions for different functions.

System Flags for TLS

Flag	Description	Manual Add Required?	Reset Required?
ENABLE_TLS_V_1_0	After setting the value to YES, central signaling and LDAP communication will fall back to TLS 1.0. Default value: NO Note: Enabling the above flag will not stop TLS 1.2 to work. Initiating communications will be with TLS v1.2 protocol.	Yes	Yes
RMX_MANAGEMENT_SECURITY_PROTOCOL	• After setting to TLS1_2_TLSV1_1_TLSV1, Apache is able to speak on TLS 1.0, TLS 1.1 and TLS 1.2. • After setting to TLSV1_SSLV3, Apache only speaks on TLS 1.0 Default: TLS1_2_TLSV1_1_TLSV1		

If the TLS 1.0 is not enabled, then TCP connection will be broken with entity that tries to communicate with RealPresence Collaboration Server.

Version 8.6.4 Detailed Description of Changed Feature

Polycom® RealPresence Clariti™ Support

RealPresence Collaboration Server 1800/Virtual Edition is available as part of Polycom® RealPresence Clariti™, a Polycom collaboration infrastructure offer that features simplified concurrent user licensing and add-on options. RealPresence Clariti customers should consult with their Polycom representative to ensure they have the correct licensing information before upgrading.
The RealPresence Clariti solution requires the Polycom® RealPresence® Platform Director™ system to license and monitor the RealPresence Collaboration Server, Virtual Edition and to monitor RealPresence Collaboration Server 1800. RealPresence Collaboration Server 1800 is still licensed in the old way as in previous releases.
The RealPresence Platform Director system is available for download at **Documents and Downloads** at Polycom Support at no additional charge

Note: Upgrade the RealPresence Platform Director System to version 3.0
If you are a RealPresence Clariti customer, you must upgrade your RealPresence Platform Director system to version 3.0 before you upgrade your RealPresence Collaboration Server 1800/Virtual Edition.

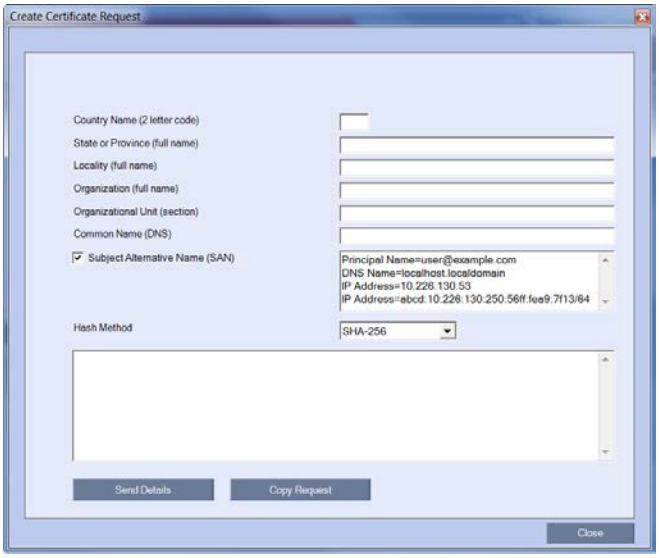
In the solution, RealPresence Collaboration Server 1800/Virtual Edition enables itself with full capacity but the real capacity still relies on other RealPresence Clariti components, for example RealPresence DMA. For installing and licensing instructions of RealPresence Collaboration Server 1800/Virtual Edition, refer to *RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Getting Started Guide*.

Version 8.6.2 Detailed Description of New Features

- New Certificate Signing Request (CSR) Guideline
- Suppress Conference Operator's Entry Tone
- REST API
- RealPresence® Media Suite/Capture Server Dial-In Collaboration Server through H.323

New Certificate Signing Request (CSR) Guideline

You can add an Management and Signaling Certificates through **Setup** > **RMX Secured Communication** > **Certification Repository** > **Personal Certificates** dialog box.
The only Certificate Method you can selected for adding Management and Signaling Certificates is **CSR**, then you can create a new certificate request by entering following attributes according to the new CSR guidelines:



Common Name (DNS): Your network administrator may have specific requirements for the content of these fields. The field is empty by default. In the absence of any other guidance, it is recommended that the following information be contained in this field:

- If DNS is being used, enter the DNS Fully Qualified Domain Name (FQDN) of the Collaboration Server Management Network Interface. This should match the Host Name and Domain configured in the Management Network Properties dialog box.
- If DNS is not being used in your deployment, enter the IP Address of the Collaboration Server Management Network Interface.

Subject Alternative Name (SAN): This field is required when using EAP-TLS in conjunction with a Network Policy Server (MS-NPS), you can fill up to 20 SANs. The field is selected by default, and when it is selected, you can modify the example values provided, to match local certificate requirements and delete

those that are not applicable.

- Principle Name: The default example will display as below:

  `Principle Name=user@example.com`

- DNS Name: If DNS/MCU Host name is configured, the configured name will display, otherwise a default example will display as below:

  `DNS Name=myhost.example.com`

  Replace `myhost.example.com` with either FQDN of the Collaboration Server Management Network Interface or the MCU Host name.

- IP addresses:
  - If RMX is configured with IPv4, then the IPv4 address will display.
  - If RMX is configured with IPv6, then the IPv6 address will display, besides you can also enter additional IPv6 addresses.
  - If RMX is configured with both IPv4 and IPv6, then both IP addresses will display.

Following is a complete example as your reference:

Example:

```
DNS Name=rmx1.polycom.com
IP Address=10.11.12.13
IP Address=fe80::592f:6a4c:87b:b69a
IP Address=fe80::2e0:dbff:fe0b:f9e4
```

If an incorrect SAN type is entered, an error message, Unsupported SAN type, is displayed when the **Send Details** button is clicked.

The SAN field option - DNS Name (FQDN) is not used for Machine Account validation. For example, the DMA will not validate the Collaboration Server unless the FQDN field in the User Properties dialog box is correctly filled in.

Hash Method: Select the output value for the Secure Hash Algorithm:

- **SHA-256**: the output value is 256 bits.
- **SHA-1**: the output value is 160 bits.

For backward compatibility, with previous versions, either SHA-1 or SHA-256 can be selected as the hash algorithm used in the creation of CSRs.

Suppress Conference Operator's Entry Tone

Entry Tone can be used as notification of participant joining or leaving the conference.
In version 8.6.2, there is a new system flag IVR_ROLL_CALL_SUPPRESS_OPERATOR to suppress entry/exit tone when the operator participant joins or leaves the conference if the system flag is set to YES.

REST API

In version 8.6.2, Polycom RealPresence Collaboration Server supports an additional REST (REpresentational State Transfer) API resource.

This mechanism uses the REST API interface as used across Polycom RealPresence Platform solution/products. For the Collaboration Server REST API documentation, see insert site.

The changes in the REST API support are described in the table below.

RMX REST API Modifications

RMX Property	Resources	Methods	Addition/Modification	Platforms
SNMP configuration	https://localhost:8443/api/rest/snmp-config	GET	Reads the current SNMP configuration.	All MCUs
		PUT	Sets the current SNMP configuration.	

Note: plcm-snmp-config Important Stipulations

- The following parameters are ignored:
  - plcm-snmp-config-minimum-notification-interval-v2
  - plcm-snmp-config-pass-list-v2
  - plcm-snmp-config-trap-sinks-v2
- Trap configuration requires the ported used is 162, and transport-type is “UDP”. Any other values result in transaction rejection.

  Queries configuration allows other values for port and transport-type (i.e.”TCP”).

The table below summarizes the elements currently supported by the RMX.

RMX REST API supported functionalities

RMX Property	Resources	Methods	Functionality Description	Platforms
External CDRs **plcm-cdr-client-config**	https://localhost:8843/api/rest/config/cdr-client-config	GET PUT	CDR server configuration (IP/name, port, username, password, etc.)	All MCUs
NTP **plcm-time**	https://localhost:8443/api/rest/config/time-config	GET PUT	Time settings (enable/disable NTP, list of NTP servers)	All MCUs

RMX REST API supported functionalities

RMX Property	Resources	Methods	Functionality Description	Platforms
Licensing server (FLEXERA) **plcm-license**	https://localhost:8443/api/rest/config/licenses/refresh-licenses	POST	Licensing server configuration (IP/name, port, and authentication information).	Virtual Edition
	https://localhost:8443/api/rest/config/licenses/authority-config	PUT	License refreshing.	
	https://localhost:8443/api/rest/config/licenses/license-status	GET	Returns the license status and associated features associated with this product.	
SNMP configuration **plcm-snmp-config**	https://localhost:8443/api/rest/snmp-config	GET PUT	SNMP configuration (product, SNMP version, transport type, port, authentication method, encryption method, security user list, etc.)	All MCUs

RealPresence® Media Suite/Capture Server Dial-In Collaboration Server through H.323

RealPresence Media Suite/Capture Server dialing in Collaboration Server through SIP was supported in previous releases.

In version 8.6.2, RealPresence Media Suite/Capture Server dialing in Collaboration Server through H.323 is supported, and its configurations remain the same with RealPresence Media Suite/Capture Server dialing in Collaboration Server through SIP shown as below:

- Enabling the Recording Features in a Conference IVR Service

  For more information, refer to *RealPresence Collaboration Server 1800/2000/4000/Virtual Edition Administrator Guide*.
- Enabling the Recording in the Conference Profile

To enable recording for a conference:

1. In the **Collaboration Server Management** pane, click **Conference Profiles**
2. Create a new profile by clicking **New Profile**, or modify an existing profile by double-clicking or right-clicking an existing profile and then selecting **Profile Properties**.
3. In the **New Profile** dialog box, click the **Recording** tab.
4. Select the **Enable Recording** check box.

5 Define the following parameters:

Conference Profile Recording Parameters

Parameter	Description
Enable Recording	Select to enable Recording Settings in the dialog box.
Start recording	Select one of the following: • **Immediately** – conference recording is automatically started upon connection of the first participant. • **Upon Request** – The operator or chairperson must initiate the recording (manual).
Audio Only	Select this option to record only the audio channel of the conference. **Note:** An Audio Only Recording Link cannot be used to record a conference if there are no Voice resources allocated in the Video/Voice Port Configuration.
Display Recording Icon	Select this option to display **Recording Indications** to all conference participants informing them that the conference is being recorded. The recording icon is replaced by a **Paused** icon when conference recording is paused.
Play Recording Message	Selected by default. A message is played to all participants announcing that the conference is being recorded. Uncheck this box to prevent the announcement from being played.

6 Click **OK**.

After the recording is enabled, Media Suite/Capture Server can dial in Collaboration Server conference either for recording or playback. Media Suite users can dial in the conference either through Media Suite User Portal or Media Suite Admin Portal.

After the Collaboration Server gets the request from Media Suite/Capture Server, the recording or playback will start. During the call, you cannot switch over between recording and playback, but you can pause and stop the recording or playback from the Media Suite/Capture Server.
From RMX version 8.6.2, if the **Display Recording Icon** is selected, the H.323 conference will display an identical recoding indicator( ) as it does in a SIP conference on the up left corner of the conference layout. For more information about how to start a recording or playback from Media Suite, refer to the *Polycom RealPresence Media Suite User Guide* or *Polycom RealPresence Media Suite Admin Guide or Polycom RealPresence Capture Server User Guide*.

Version 8.6 Detailed Description of New Features

Lync Features

Version 8.6 main addition relates to Lync-related features, of which the most significant is the RealConnect technology expansion to remote premise scenarios via a Service Provider.

The features in that category are:

- New RealConnect Topology for Service Provider
- Wait for Chairperson when Collaboration Server is in Lync AVMCU Lobby
- Reestablishing Connection via DMA to AVMCU Following Collaboration Server Failure
- DNS Load Balancing on Lync Front End Pool
- Support for Skype for Business

New RealConnect Topology for Service Provider

Polycom® RealPresence® Collaboration Server 8.6 introduces a new RealConnect® federation mode, which enables both Lync and non-Lync endpoints to participate in Lync-initiated meetings, even in scenarios where those endpoints reside in remote Lync organizations.

The RealConnect mode provides a mechanism whereby a conference hosted on the Collaboration Server is capable of connecting a Lync meeting scheduled in a remote Lync organization via the RealConnect federation mode. This capability allows people in various and remote Lync-deployed organizations, to schedule Lync meetings from their respective organizations, where the meeting participants can join the scheduled meeting via a Lync-enabled RealPresence Platform (RPP), using the conference connection data included in the standard Outlook Lync meeting invite. In these conferences, participants connected via the RPP enjoy Polycom's prime conferencing experience, whereas the Lync participants enjoy a wholly Microsoft Lync conferencing experience.

In inter-organization scenarios RealConnect utilizes the Trusted Application Relationship, which is available only within the same organization. RealConnect for remote-premise scenarios, involves a new mechanism bypassing the necessity in the Trusted Application Relationship, and utilizing the Conference Auto Attendant (CAA) service. Thus, it allows the Collaboration Server to use the Lync Edge server either at the Service Provider or at the federated organization (depending on the RPP location) to connect to the remote Lync (AV MCU) meeting.

In addition, it is required to create a mechanism for identifying the various organizations involved in Lync meetings (see Organization Identification).

The Collaboration Server uses ICE over IPv4 to connect to the AV MCU.

Organization Identification

In multiple tenant scenarios, the DMA maintains a prefix table, in which each Federated organization is allocated a unique prefix, mapped to the respective organization initiating the meeting by its CAA's SIP URI.

In single tenant scenarios, since the conference ID, is unique only within the Lync server which allocated it, a prefix is added to the conference ID to enable the DMA to identify remote RealConnect Lync conferences.

The Lync service administrator of an organization hosting Lync meetings, can add the respective organization prefix into the Outlook meeting invites sent by meeting organizers. This insertion requires the Lync service administrator to configure the added text only once, via the Lync conference template, at the point of the RealConnect service deployment.

For more information on CAA SIP URI and Organization Prefix, see Polycom Microsoft Deployment Guide.

Content Sharing Support

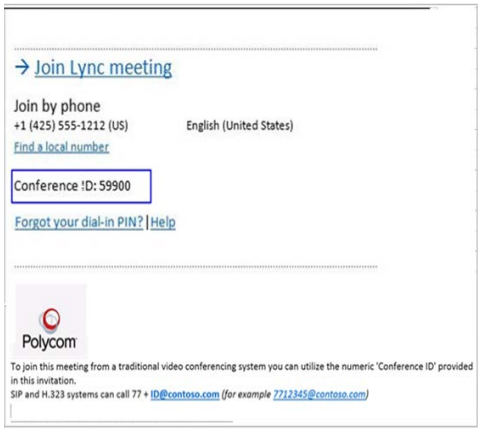
As part of supporting video conferencing in a Polycom-Lync environment, Polycom supplies Polycom® ContentConnect® for Microsoft Lync environments (previously known as Content Sharing Suite, or CSS), which enables content sharing between Lync and non-Lync conference participants.

During content sharing, content is sent from the Collaboration Server via H.264 to the ContentConnect server, and from there via Microsoft Remote Desktop Protocol to the Lync AV MCU, and vice versa.

For more information on ContentConnect, see Deployment Into Microsoft Environments, Sharing Content During a Conference, in the *RealPresence Collaboration Server Administrator Guide*.

Process Guidelines

- To overcome the absence of a Trusted Application Relationship, the DMA utilizes the Microsoft CAA service.
- Lync Meeting invites include the Lync conference ID, and at the bottom, the prefix of the federated organization.



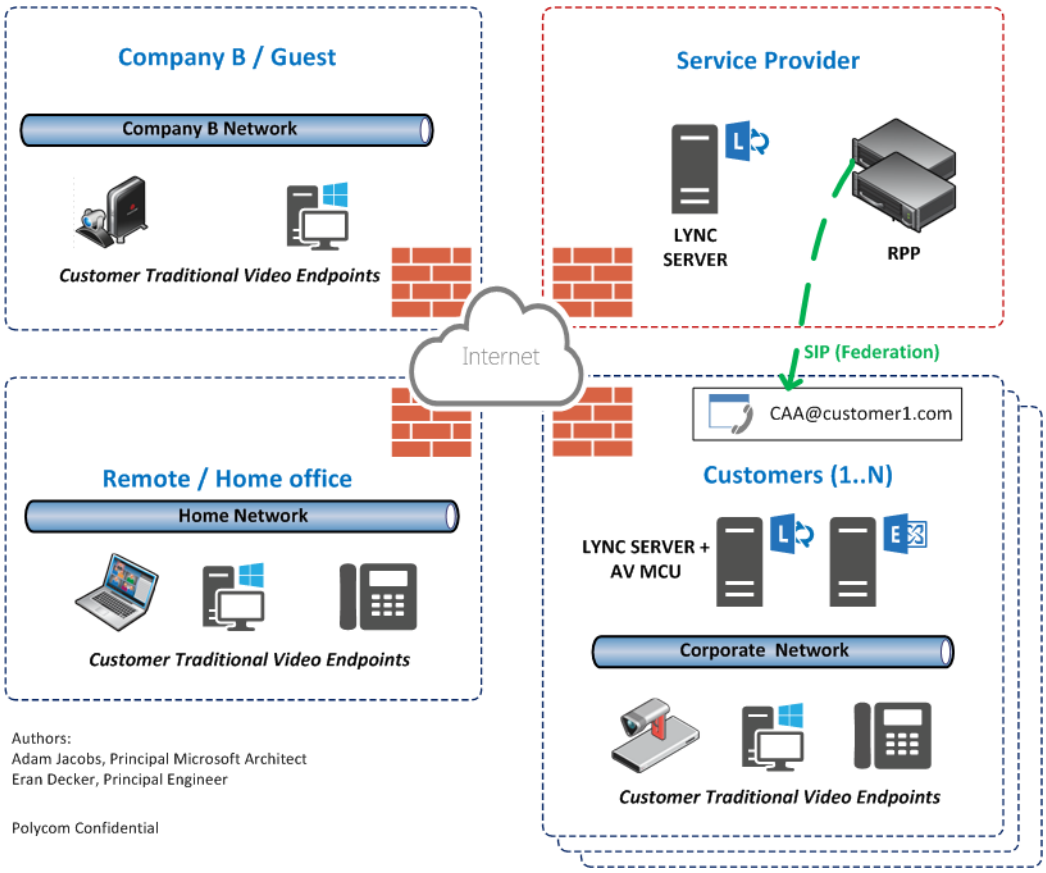
- The RealConnect connection is established within 7 seconds, at the most.
- The audio/video of non-Lync participants is muted/suspended during the process, so as to keep the RealConnect process hidden.

  Once RealConnect of Collaboration Server and AV MCU conferences is complete, non-Lync participants may receive audio/video depending on conference configuration (i.e., if dependent on chairperson presence).

Supported Deployment Topologies

Polycom supports the deployment topology illustrated below.

- Multi-tenant, each owning its own CAA Service, and using an independent Service Provider containing the RPP solution. In this constellation, the DMA maintains an organization prefix table, with each prefix linked to the organization CAA Service URI.



Error Handling

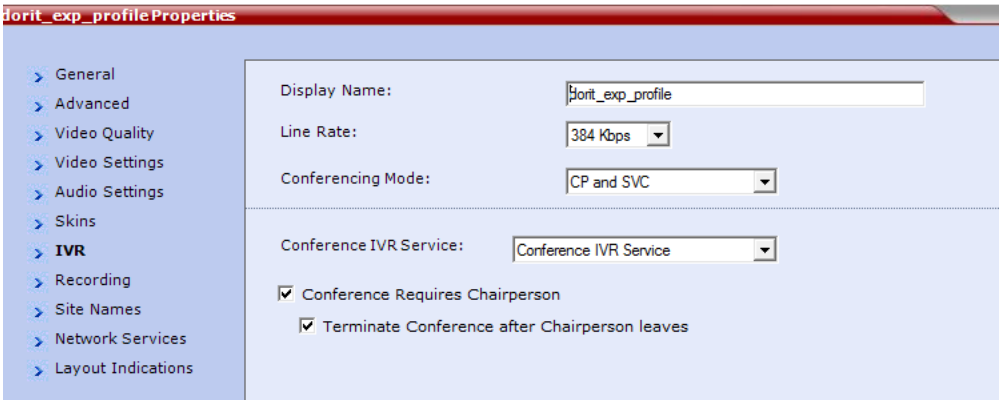
- If the federated organization prefix entry in the DMA table yields an erroneous CAA URI, the participant is immediately disconnected.
- If a non-Lync endpoint dials an erroneous number as the conference ID on the AV MCU, the participant is immediately disconnected.

Wait for Chairperson when Collaboration Server is in Lync AVMCU Lobby

In Microsoft Outlook, you can determine that all the participants in the conference should await the Organizer in the AV MCU lobby. This feature in AV MCU is, in fact, the equivalent of Collaboration Server

chairperson concept, where participants await the chairperson presence before the conference can begin, depending on conference/profile configuration.

From 8.6, in a cascading conference, where the Collaboration Server cascaded link is awaiting the Organizer attendance in the AV MCU lobby, the participants connected to the Collaboration Server will also await his presence in the lobby, provided the conference profile is configured to begin upon first chairperson connecting (first check-box below), either by DMA via API specification, or by the Collaboration Server Administrator user following DMA request to use a certain profile with this option set.



The purpose of this is to maintain conferencing stability, which suffered in the past due to discrepancy between Lync and the Collaboration Server conferencing chairperson settings. It also prevents mis-usage of Polycom VMR and conferencing services during the two weeks following the meeting, which was possible due to Lync keeping the meeting VMR open for that duration, thus allowing its unauthorized re-usage.

If the conference is configured to be without a chairperson, the participants connected to the Collaboration Server can freely view and hear each other, whereas the participants connected to the AV MCU have both video and audio muted.

Once the Organizer leaves the conference, the conference should not end automatically. Instead the Collaboration Server should imitate the client behavior.

If the cascading link to the AV MCU is disconnected, the Collaboration Server should follow the conference configuration, meaning, terminate the conference only if the **Terminate Conference after Chairperson leaves** (second check-box in the figure above).

The AV MCU cascaded link is considered as chairperson, resulting in the participants connected to the Collaboration Server awaiting the connection to AV MCU in the lobby, with no actual chairperson required on the AV MCU side or at an endpoint.

The Master AV MCU participant will have a chairperson icon ( ) attached to its name in the Collaboration Server conference participants screen.

Since chairperson password is not supported in Microsoft Outlook, it is bypassed by exploiting the fact, that the Collaboration Server does not request a chairperson password if the conference password was entered. Therefore, the DMA generates a conference password, and uses this password when calling all the participants in the conference, which in turn use it to connect the conference, without the chairperson password being required.

All ContentConnect (Polycom content sharing for Microsoft environments) related actions begin only after the Collaboration was moved from the AV MCU lobby into the conference.

Reestablishing Connection via DMA to AVMCU Following Collaboration Server Failure

Polycom RealPresence Collaboration Server supports conferencing with Microsoft Lync clients via a VMR in the DMA, where the Collaboration Server is connected through a cascading link to Microsoft AV MCU. Should the Collaboration Server fail, the DMA containing the VMR to which both MCUs were connected, is capable of recreating the conference on an alternate Collaboration Server.

To complete this capability, from version 8.6 and on, the DMA has the added capability to re-establish the cascading link to the AV MCU as well. This is done by the Collaboration Server providing the AV MCU Focus (SIP) URI to the DMA, as part of the conference information, even for Ad-Hoc conferences.

In addition, two additional values are passed via the XML API from the Collaboration Server to the DMA within the conference information, to enable proper termination of the recreated conference (as explained in the conference termination below):

- The original AV MCU conference type - scheduled (AV MCU), scheduled (PCM), Ad-Hoc, or none (meaning non-AV MCU conference).
- The value of the “To” field in the original invitation.

Cascading Conference Reestablishment Process

1. Once the DMA detects a Collaboration Server failure (via XML API or ping), it disconnects all the Collaboration Server SIP connections (legs) except the SIP connection to the AV MCU.
2. The DMA recreates the conference on an alternate Collaboration Server, and passes to it (via XML API) the AV MCU Focus URI, the conference type, and the value of the original “To” field in the Microsoft invite, as preserved from the original conference.
3. The Collaboration Server uses the Focus URI to recreate the cascading link to the AV MCU, and recreates the conference using the conference type retained from the original conference.
4. The Collaboration Server uses the original “To” field value to create SIP sessions to the “leftover” SIP connections from the AV MCU to the original Collaboration Server in order to disconnect them.

Reestablished Cascading Conference Termination

Once all the Collaboration Server participants are disconnected, the Collaboration Server uses the retained conference type to determine whether or not the cascading link to the AV MCU should be disconnected:

- For scheduled conferences - The cascading link is disconnected.
- For Ad-Hoc conferences - The cascading link is not disconnected.

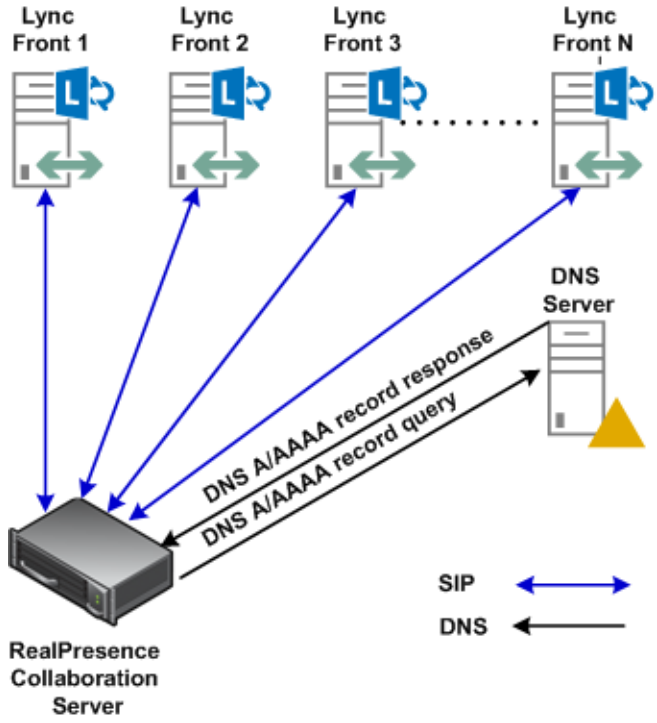
DNS Load Balancing on Lync Front End Pool

In the Lync environment, the Front End server is the SIP server, Focus server and A/V MCU.

Polycom® RealPresence® Collaboration Servers 1800/2000/4000, and Virtual Edition, support DNS load balancing that balances the SIP traffic to maximum up to 12 Front End servers in the same Front End Pool.

The Collaboration Server supports DNS load balancing on Lync Server 2010 and Lync Server 2013.

Following figure shows how the Collaboration Server supports DNS load balancing.

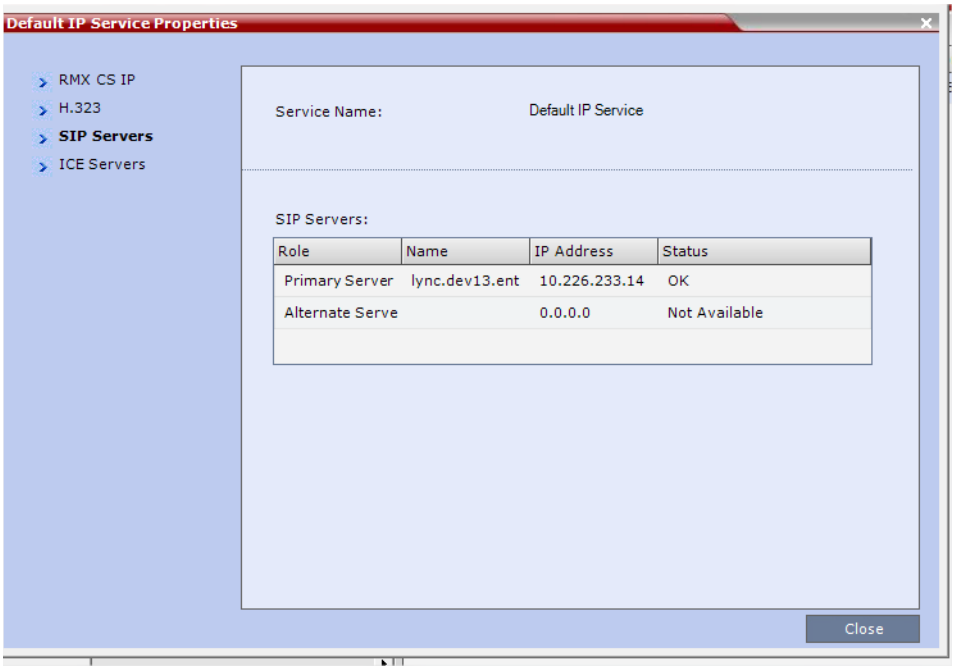


All Front End (FE) servers in the pool register themselves in DNS server with the same FQDN but different IP addresses (both IPv4 and IPv6 are supported).

The Collaboration Server supports both FE Load Balancing and FE Failover.

- FE Load Balancing, is implemented by the DNS server. Each DNS query is replied by the DNS server with different priorities, and the Collaboration Server connects with the FE with the highest priority.
- FE Failover, in case the Collaboration Server fails to communicate with the first FE in the DNS list, it will try and gain connection with the second FE in the list, and so on.

The Collaboration Server presents the FE IP connected in the **Default IP Service Properties** > **SIP Servers** tab as shown below:



Support for Skype for Business

All descriptions applicable for Lync 2013 are also applicable for Skype for Business.

Note: Support for Microsoft® Skype for Business

- The latest RPP versions are required.
- The Polycom product versions and the Microsoft® Skype for Business versions tested can be found in the Release Notes for Polycom Unified Communications for Microsoft Environments - June 2015 at Polycom Unified Communications for Microsoft Environments.

Ultra Secure Mode Features

The following Collaboration Servers running version 8.6 are compliant with UC APL requirements:

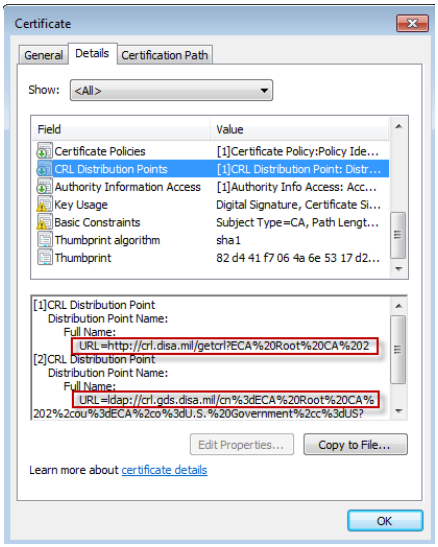
- RMX 2000/4000 equipped with MPMRx media cards
- RMX 1800

Automatic CRL (Certificate Revocation List) download from CDP (CRL Distribution Point)

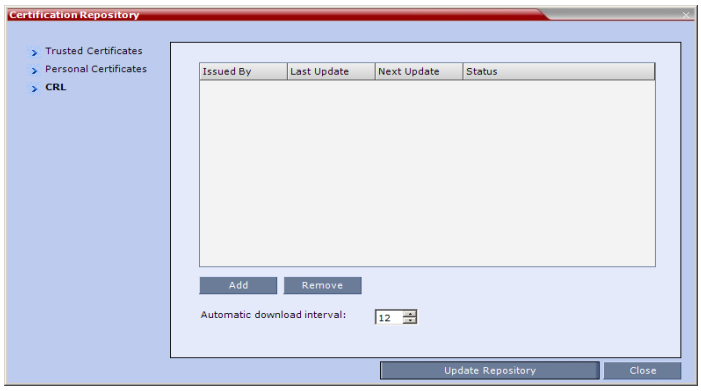
CRLs, previously manually downloaded, can now be automatically downloaded from a CDP (CRL Distribution Point). An Automatic Download Interval can be specified. Both HTTP and LDAP URIs are supported.

In previous versions there was a risk that if manual updates were not timeously performed, expired CRLs and Certificate validation failures would necessitate a system reset to delete all Certificates and CRLs, followed by re-installation of all Certificates and CRLs.

Where CAs include multiple CDPs in a Certificate, the MCU will try each URI successively until a response with a new CRL is found.



- A CRL is automatically installed when the administrator installs a CA that has an existing CDP.
- Manual installation of CRLs is supported as in previous versions.
- The MCU will always use the latest CRL if a conflict should arise.
- The automatic CRL download procedure is run after every system reset. A CRL will only be downloaded if it supersedes the current CRL.
- An Automatic Download Interval can be specified in the **Certification Repository - CRL** dialog.



➢ The Automatic Download Interval range is 0-168 hours, the default is 12. A value of 0 disables automatic CRL download.

Propagate New CRL

A new System Flag **FORCE_APACHE_REBOOT_UPON_CRL_UPLOAD** has been added to allow the administrator to choose the method of propagating a new, automatically downloaded CRL to the various Apache Server clients.

Range: YES/NO

Default: NO

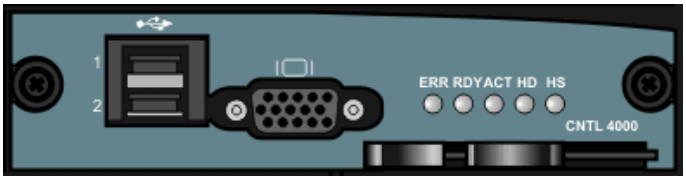
- If the value of FORCE_APACHE_REBOOT_UPON_CRL_UPLOAD is NO, the Apache Server is not rebooted when a new CRL is automatically uploaded.
- If the value of FORCE_APACHE_REBOOT_UPON_CRL_UPLOAD is YES the Apache Server will be rebooted when a new CRL is automatically uploaded.
  - Applicable to automatically uploaded CRLs only, manual CRL upload includes the option of updating the Certification Repository by rebooting the Apache Server.
  - Applies to Default Management Network Service CRL only.

If you want to modify System Flag values, the flags must be added to the System Configuration file. For more information see Modifying System Flags.

Blocked External VGA Port

In compliance with UC APL requirements, the VGA port on the RMX2000/4000 Control Modules (BRD2534B-L0 / BRD2535B-L0) are blocked when the MCU is set to Ultra Secure Mode.

Control Module with VGA Port



There is no output to the VGA port when the MCU is set to Ultra Secure Mode.

Note: BIOS Password

If a BIOS Password is required as an extra level of security, it should be established before the Collaboration Server is set to Ultra Secure Mode.

Feature Availability

The behavior of the Collaboration Server has been changed to allow less rigorous enforcement of policies and restrictions on features in Ultra Secure Mode.

Beginning with this version, the following features, previously blocked in Ultra Secure Mode are now available:

- SUPPORT User. An Active Alarm is raised when this user type is present in the system. Strong Password policy is enforced for this user, as for all other user types.
- Chairperson user.

- ISDN Cascade.
- PCM (Personal Conference Manager) interface can be used in Ultra Secure Mode. The PCM_FECC system flag determines whether the DTMF Code ##, the endpoint's remote control Far/Arrow Keys (FECC), or both will activate the PCM interface. This flag can be also be used in combination with DTMF code definitions to disable PCM.
- Web link (Hyper-link in Participant Properties dialog box).
- PCO (MS-Outlook).
- Video Preview.
- Logger Diagnostic Files can be accessed by the SUPPORT user for troubleshooting and debugging purposes. For more information see Logger Diagnostic Files.
- Information Collector files can be accessed by the administrator user for troubleshooting and debugging purposes. For more information see Information Collector.
- BFCP over TCP. For more information see Media Encryption and Authentication.
- All restrictions on Active Directory Roles have been removed.
- Multiple Content Resolutions.

Changes to the User Interface (RMX Manager)

- Display of the Login Screen and Main Screen banners of the RMX previously mandatory in Ultra Secure Mode, can be enabled or disabled regardless of the security mode setting. Bothe banners are fully customizable.
- The Secured Communication check box is selected by default in Ultra Secure Mode but can be selected or deselected regardless of the security mode setting.

New System Flags

New system flags have been added:

- SIP_BFCP_DIAL_IN_MODE—Controls BFCP's use of UDP and TCP protocols for dial-in SIP Client connections according to its value: AUTO, UDP, TCP.

  Range: AUTO / UDP / TCP

  Default (Ultra Secure Mode): UDP

  Default (normal security mode): AUTO
- ICMP_ECHO —When set to NO the system will not respond to ICMPv6 or ICMPv4 echo requests to a broadcast address. The system will also ignore ICMP (IPv4/IPv6) redirect messages, and will not t process ICMP timestamp requests.

  Range: YES / NO

  Default (Ultra Secure Mode): NO

  Default (normal security mode): YES

If you want to modify these System Flag values, the flags must be added to the System Configuration file. For more information see Modifying System Flags.

Changes to System Flags

In previous versions, when the ULTRA_SECURE_MODE system flag was set to YES, System Flags affected by Ultra Secure Mode were automatically set to their Ultra Secure Mode defaults within Ultra Secure Mode value ranges. The flags could be manually added to the System Configuration and their values modified within Ultra Secure Mode ranges. These flags and the Ultra Secure Mode policies they enforced could not be disabled or overridden.

APACHE_KEEP_ALIVE_TIMEOUT—The default value of the system flag in normal security mode has been changed to 15. The value range of the flag is 1-999. The flag remains configurable regardless of the security mode.

DEFAULT_USER_ALERT—The range of this system flag has been extended in Ultra Secure Mode to include a NO option, allowing it to be disabled.

ENABLE_ACCEPTING_ICMP_REDIRECT—The default is NO regardless of USM configuration, and the can be configured irrespective of security mode.

ENABLE_CYCLIC_FILE_SYSTEM_ALARMS—The default value of this system flag in normal security mode has been changed to NO. The flag remains configurable regardless of the security mode.

FORCE_STRONG_PASSWORD_POLICY—The range of this system flag has been extended in Ultra Secure Mode to include a NO option, allowing it to be disabled.

When FORCE_STRONG_PASSWORD_POLICY is disabled, the following system flags can be manually added to the system configuration and their values set to values within their normal security mode ranges. When FORCE_STRONG_PASSWORD_POLICY is enabled, they are automatically set to their Ultra Secure Mode ranges and default values. However, when in Ultra Secure mode the flag values can be modified within their Ultra Secure Mode ranges by manually adding them to the system configuration and modifying their values. Each flag can be individually disabled by setting its value to 0.

- DISABLE_INACTIVE_USER
- MIN_PASSWORD_LENGTH
- MIN_PWD_CHANGE_FREQUENCY_IN_DAYS
- NUM_OF_LOWER_CASE_ALPHABETIC
- NUM_OF_UPPER_CASE_ALPHABETIC
- NUM_OF_SPECIAL_CHAR
- NUMERIC_CHAIR_PASS_MAX_LEN
- NUMERIC_CONF_PASS_DEFAULT_LEN
- NUMERIC_CONF_PASS_MAX_LEN
- NUMERIC_CHAIR_PASS_MIN_LEN
- NUMERIC_CONF_PASS_MIN_LEN
- PASSWORD_EXPIRATION_DAYS
- PASSWORD_EXPIRATION_WARNING_DAYS
- PASSWORD_HISTORY_SIZE

HIDE_CONFERENCE_PASSWORD—The default value of this system flag in Ultra Secure Mode has been changed to YES.

SESSION_TIMOUT_IN_MINUTES—The range of this system flag in Ultra Secure Mode has been changed to 0-999 with a default of 10. The flag is configurable regardless of security mode. A flag value of 0 disables the flag.

Network and System Features

The Network features in the V8.6 release are:

- High CPU Usage Detection
- OpenSSL Upgrade

High CPU Usage Detection

In this version, a High CPU Usage detection and protection mechanism have been implemented on Collaboration Servers (RMX) 1800/2000/4000, and Virtual Edition platforms.

When high CPU usage, beyond a predefined threshold is detected:

- An Active Alarm is raised.
- New calls to the MCU are blocked.
- Load increasing (CPU intensive) processes within the MCU are suspended.

When CPU usage drops below the predefined threshold, the call blocks are removed and normal MCU behavior resumes.

OpenSSL Upgrade

Resolved Issues and Corrections

OpenSSL is upgraded to 1.0.1k to address multiple security vulnerabilities.

Issues Addressed by Version 8.6

Issue #	Description
CVE-2015-0206	Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.
CVE-2015-0205	The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.
CVE-2015-0204	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a non-compliant role.

Issues Addressed by Version 8.6

Issue #	Description
CVE-2014-8275	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.
CVE-2014-3572	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.
CVE-2014-3571	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.
CVE-2014-3570	The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

For more information on *Common Vulnerabilities and Exposures* see http://cve.mitre.org.

Cascading Features

Cascading features include:

- Enable Chairperson Managing Cascaded Meetings
- Snatching Content Token in Cascaded Meetings

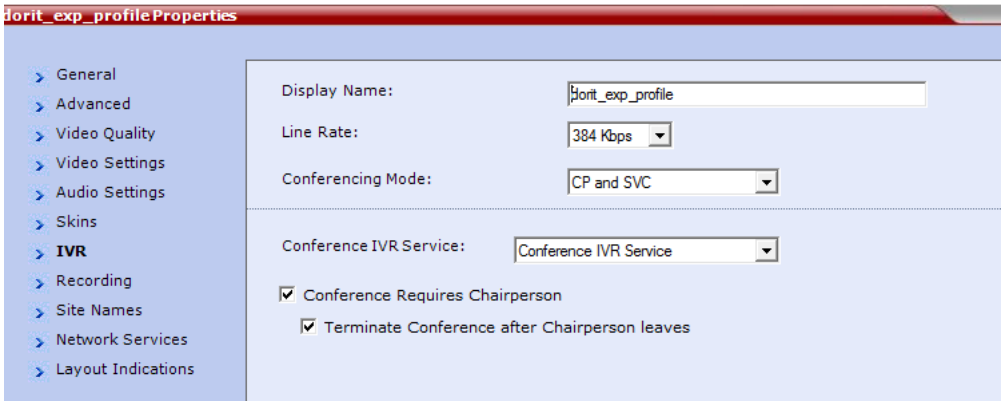
Enable Chairperson Managing Cascaded Meetings

From version 8.6 and on, a conference may be started or terminated based on a chairperson presence in any MCU within a cascading topology.

This feature depends on conference profile configuration as shown in the figure below:

- The conference begins upon first chairperson connecting (first check-box).

- The conference terminates upon last chairperson disconnecting (second check-box).



Process Description

Once a chairperson connects an MCU in the cascading topology, the conference begins locally at this MCU.

The DMA polls (via API), from all the MCUs in the cascading topology, information on the cascading conference and its participants, which includes information of chairperson participants. The DMA sends the conferences information to all the MCUs, registered for conference notifications (via EventPackage).

Through these notifications each of the subscribed MCUs can determine the point at which the first chairperson joins the conference, and begin transmitting the conference audio/video to the connected participants. Similarly, each MCU can determine at which point the last chairperson disconnects from the conference, and terminate the conference.

During the conference, a new MCU may link to the cascading conference. This MCU subscribes to the DMA for conference notifications. Should a chairperson be connected to the conference on that MCU, this chairperson presence is passed (as explained above) to the other MCUs in the cascading topology, so each of the MCUs can process the information and act accordingly.

The DMA server used for subscribing to the EventPackage conference notifications is reached using a URI, obtained by the MCU through the XML API.

Chairperson in Cascading Environment Guidelines

- The IP network service related to the conference should support SIP:
  - The IP network service and the EventPackage use the same transport type.
  - It is recommended not to use UDP as transport type.
- Participants connecting the conference via a gateway, are required to enter the chairperson password in order to be considered chairperson.

Error Handling

The following error handling measures are taken:

- If the EventPackage SIP connection to one of the MCUs fails to establish following 3 consecutive attempts, that MCU generates an active alarm specifying the specific conference and VMR. This alarm is cleared upon conference end. The failing MCU will join the conference based on a local chairperson presence, instead of anywhere within the cascading topology.

- On the off chance that one of the cascaded links breaks, EventPackage functionality continues, and connected MCUs continue based on the EventPackage notifications. Possible unexpected behavior due to this broken link may occur.

Snatching Content Token in Cascaded Meetings

From version 8.6 and on, content can be snatched in cascaded environments, that is the content token ownership can be taken/snatched by another participant wishing to share content where content is currently shared by another participant.

This capability depends on the conference configuration (Exclusive Content Mode is off), and the ENABLE_CONTENT_SNATCH_OVER_CASCADE system flag (described below).

Guidelines for Content Snatching in Cascaded Conferences

- Content Snatching is available only over anH.323 cascaded link. It is not applicable to either SIP (BFCP) or PSTN.
- All the MCUs within the (H.323) cascading topology should:
  - Use RealPresence Collaboration Server version 8.6 and up.
  - Have Exclusive Content Mode turned off (meaning, **Exclusive Content Mode** check-box in conference profile **Properties > Advanced** tab should be cleared).
  - Have the system flag **ENABLE_CONTENT_SNATCH_OVER_CASCADE** value set to **YES**.

When a Master MCU is not in Exclusive Content Mode, another participant in the same MCU may snatch the content, even if the value of the **ENABLE_CONTENT_SNATCH_OVER_CASCADE** system flag is **NO**.

System Flag

When the **ENABLE_CONTENT_SNATCH_OVER_CASCADE** system flag value is **YES** in all the MCUs within the H.323 cascaded topology (and assuming all MCUs are using Collaboration Servers version 8.6 and up), content snatching is enabled.

Default value: **NO**.

To set the flag value to **YES**, it is required to manually add it to the system configuration flags, and modify its value to **YES**.

No system restart is required for flag modified value to take effect.

Hardware Features

A new platform is introduced in version 8.6, Polycom RealPresence Collaboration Server, Entry Level. Its description can be viewed in New Entry Level RealPresence Collaboration Server 1800 for Japanese Market

Further Hardware features are:

- MPMx Excluded from Version 8.6
- Reset MPMRx Media Card
- High CPU Usage Detection

New Entry Level RealPresence Collaboration Server 1800 for Japanese Market

From version 8.6, Polycom® seeks to replace the previous RealPresence® Collaboration Server 1500 SMB platform, which was created specifically for the Japanese market as a solution for small-scale businesses, with RealPresence Collaboration Server 1800, Entry Level, with one DSP card.

This platform capabilities are mostly similar to those of Collaboration Server 1800 with 1 DSP card, with some of the features unsupported.

Below, is a description of the supported features and platform capabilities.

Feature Support

This Collaboration Server supports most of the features supported by the general product, as is summarized in the following table:

Feature Supported by Collaboration Server 1800, Entry Level, with one DSP card

Feature	Comments / Limitations
Max supported concurrent conferences	90
Unified conferencing (voice, video, and content)	See below
Audio	
Audio codecs - G.711a/uG.722, G.722.1C, G722.1, G.723.1, G.719, G.729A, Polycom® Siren™ 14, Siren 22	The last two - in mono or stereo
Advanced IVR flow	
IVR prompts for auto attendance	
DTMF support	
User and manual mute control	
Echo and keyboard noise suppression	
Audio Clarity	
Selective audio mixing	
Video	
Standard H.264 High Profile	
Conferencing video aspect ratios	16:9 and 4:3
Customized resolution configuration	Beginning with QCIF and up to HD1080p30 (in VSW conferences; in CP conferences - up to HD720p30)
Protocols	• H.264 (HP) AVC • H.263 (++)
CP transcoding	Up to 720p30.

Feature Supported by Collaboration Server 1800, Entry Level, with one DSP card

Feature	Comments / Limitations
Content	
Content sharing over H.239	
Content protocols	H.263 and H.264
Polycom® People+Content™ technology	
Conferencing Features	
Conferencing Modes	AVC - CP and VSW
Lecture and Presentation modes	
Conference Dial-In/Out	
Conference Profiles & Templates	For easy establishment of recurring conferences.
Meeting rooms	Up to 1000
Up to 26 different layouts	Layouts range: 1x1 to 4x5. **Note:** Same as 1800 with one DSP card.
Layout background (skin) configuration	
Message Overlay	
Multilingual and transparent site name options	
Integration with Polycom® Capture Server™ for recording and streaming	
Polycom® Click&View™ visual layout tool	
FECC (Far-end Camera Control)	H.224 / H.281, H.323 Annex Q, and SIP FECC
Customized HD Welcome slides	
Roll Call	
Closed caption	
System, Management, and Hardware	
Redundant power supply (optional add-on)	
Access	• Web-based - RMX Web Client • Application-based - RMX Manager
Multi Collaboration Server management	Up to 10 Collaboration Servers may be controlled via the RMX Manager
Users	Administrator, Operator, Chairperson, Auditor, each with respective authorities
Operator conference	Including moving participants between conferences

Feature Supported by Collaboration Server 1800, Entry Level, with one DSP card

Feature	Comments / Limitations
SNMP V3.0 for external monitoring	
Network Support and QoS	
IP H.323	AVC
IP SIP	AVC
Addressing modes	IPv4 and IPv6
10/100/1000 Mb interface	
Conference data rates	Beginning with 64 Kbps and up to 6 Mbps (in VSW; in CP up to 4Mbps)
Dial-in method	Direct dial-in from all networks
IP Qos and precedence	
Polycom LPR (Lost Packet Recovery)	Both H.323 and SIP protocols
DiffServ	
Dynamic jitter buffer	
Audio/video error concealment	
Security	
AES media encryption	IP
TLS (Transport Layer Security)	SIP and management network
Strong password policy	
Tiered administrative access level	
Secure conferencing mode	

System Capabilities

Capabilities of Collaboration Server 1800, Entry Level, with one DSP card

Element	Capability
Conferencing Modes	CP, VSW
Maximum resolution	• VSW - 1080p30 • CP - 720p30
Maximum number of ports	15 720p30 ports **or** 180 audio ports
Maximum number of simultaneous conferences	90
Maximum number of video participants in CP conference	30

Capabilities of Collaboration Server 1800, Entry Level, with one DSP card

Element	Capability
Maximum number of audio-only participants in CP conference	180
Maximum number of video call per second	2
Maximum number of audio call per second	5
Maximum number of Meeting Rooms	1000
Maximum number of Entry Queues	40
Maximum number of Profiles	80
Maximum number of Templates	400
Maximum number of SIP Factories	40
Maximum number of IP Services	2
Maximum number of IVR Services	80
Maximum number of Recording Links	20 (default)
Maximum number of IVR video slides	150
Maximum number of CDR files	2000
Maximum number of Fault files	1000
Maximum number of Participant alerts	None - Unlimited
Maximum number of simultaneous Web Client connections to a single Collaboration Server 1800 Entry Level.	20
Maximum number of Users	100
Port configuration	One of: • 5/10/15 H.264/720p ports • 10/20/30 SD/VSW
Box level redundancy	None
RealPresence RMX Manager	Yes
Maximum line rate	• CP - Up to 4Mbps • VSW - Up to 6Mbps

System Capacities

Capacities of Collaboration Server 1800, Entry Level, with one DSP card

Resolution	Max Line Rate	Target Capacity	Comments
AVC			
720p30	2M	15	Standard port. **Note:** 4M rate for 720p30 is also supported, but with lower capacity (about 1.5 ports)
SD	1M	30	Resource - 0.5 port
CIF	1M	30	
H263 CIF	1M	15	Same as 720p30
H263 SD	1M	15	
H264 CIFp60	1M	15	
H264 SD/4CIFp60	2M	15	
VSW			
1080p30	6M	30	
1080p30	4M	30	
1080p30	2M	30	
Audio			
Audio only	-	180	Based on 1:12 ratio

Licensed Capacities

Licensed Capacity - Collaboration Server 1800 Entry Level, with one DSP card

Licenses	CP 1080p60	CP 1080p30	CP 720p30	CP SD	CP CIF	Audio
5	N/A	N/A	5	10	10	60
10	N/A	N/A	10	20	20	120
15	N/A	N/A	15	30	30	180

Port Ratios

Port Ratios - Collaboration Server 1800 Entry Level, with one DSP card

Licenses	CP 1080p60	CP 1080p30	CP 720p30	CP SD	CP CIF	Audio
5	N/A	N/A	1.00	2.00	2.00	12.00
10	N/A	N/A	1.00	2.00	2.00	12.00
15	N/A	N/A	1.00	2.00	2.00	12.00

MPMx Excluded from Version 8.6

From version 8.6, the MPMx media card is no longer supported, and with it, Collaboration Server 1500.

Upgrading is prevented if the source version is one of:

- 8.4.2HF (FSN-829)
- 8.5.2HF
- 8.5.3 and up.

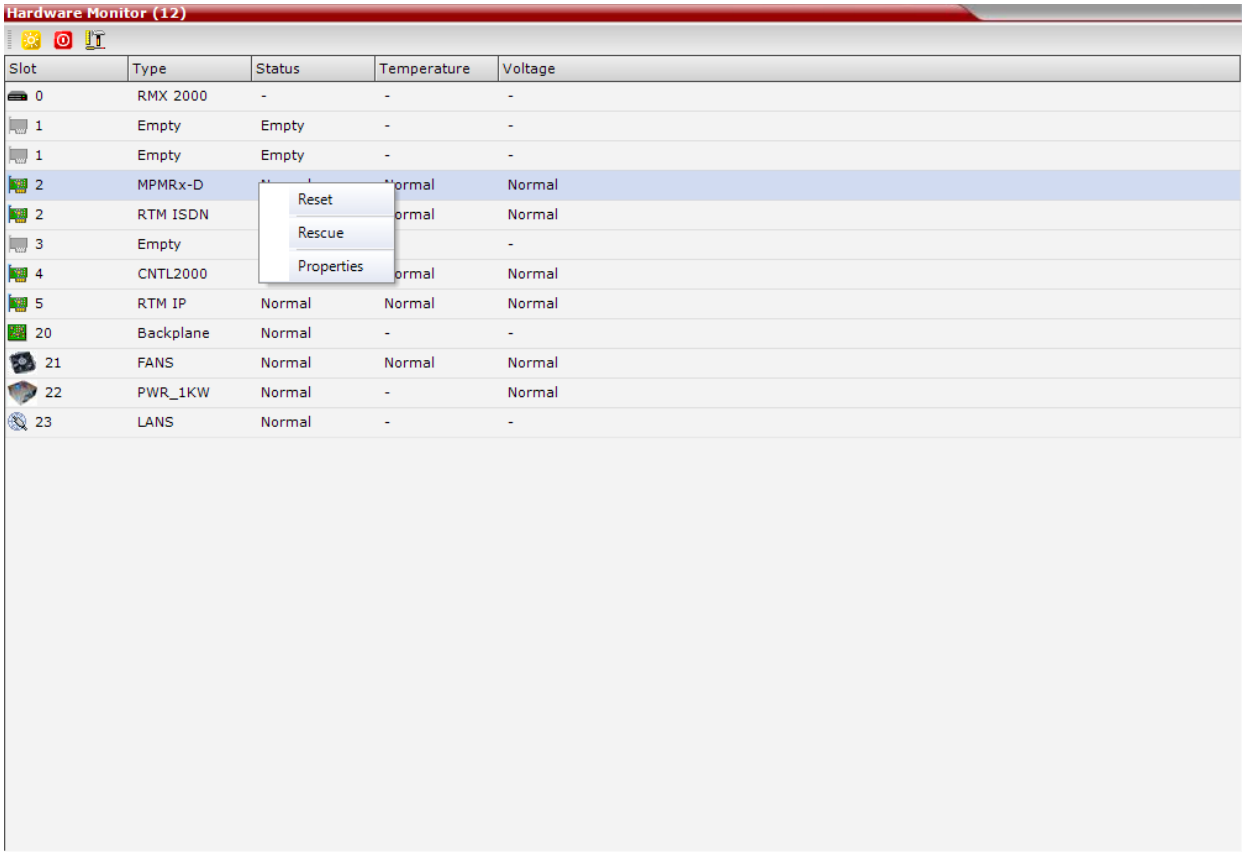
Upgrade from other versions succeeds, though an active alarm appears, indicating that “The card type in slot <*n*> is not compatible with RMX version, card will not be powered on”.

Reset MPMRx Media Card

From version 8.6, when an MPMRx card crash occurs, you can reset the MPMRx Media cards via the **Hardware Monitor** pane by right-clicking each MPMRx Media card and selecting **Reset.**

Note: Resetting MPMRx Media card
Only users with Support permission can reset an MPMRx Media card.

The card reset process in performed within two minutes.



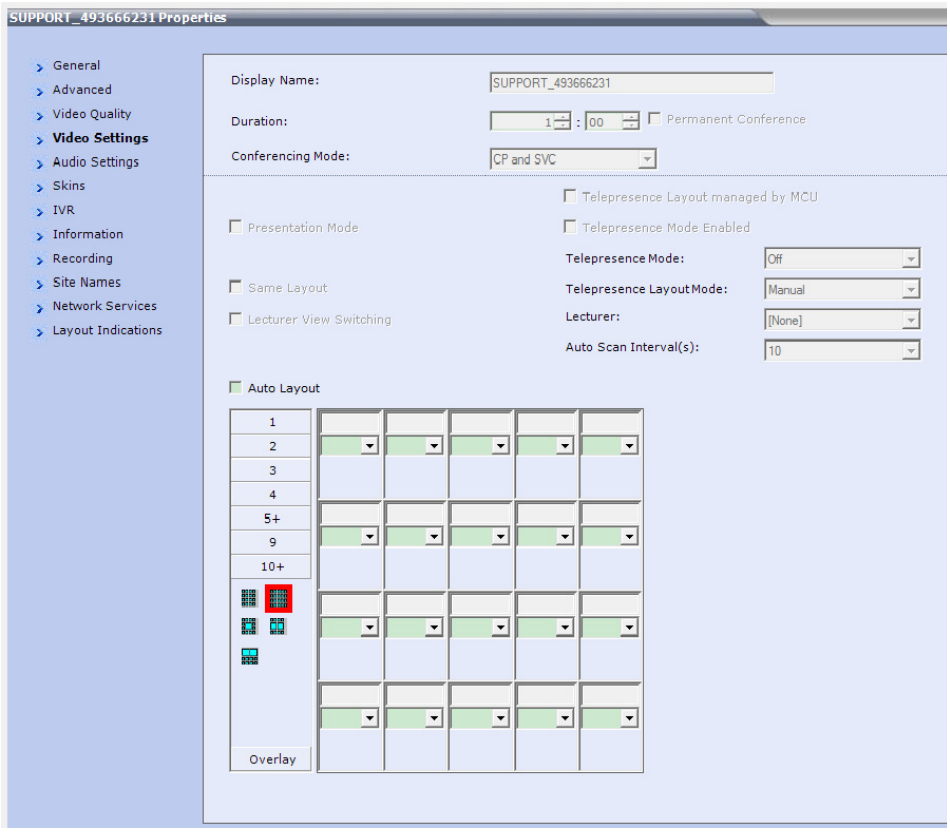
Miscellaneous Features

General features added to V8.6 are:

- New 4x5 Layout
- Video Participants Indication
- Change SVC License ratio to 1:5
- Configuration option to disable G.729

New 4x5 Layout

Collaboration Servers 1800/2000/4000, and Virtual Edition support a new 4x5 layout. The 20 cells layout can be customized in AVC conference and CP and SVC mixed conference.



Video Participants Indication

From version 8.6, Polycom® RealPresence Collaboration Server provides AVC endpoints with indication on both the presence and the number, of video participants connected to the conference.

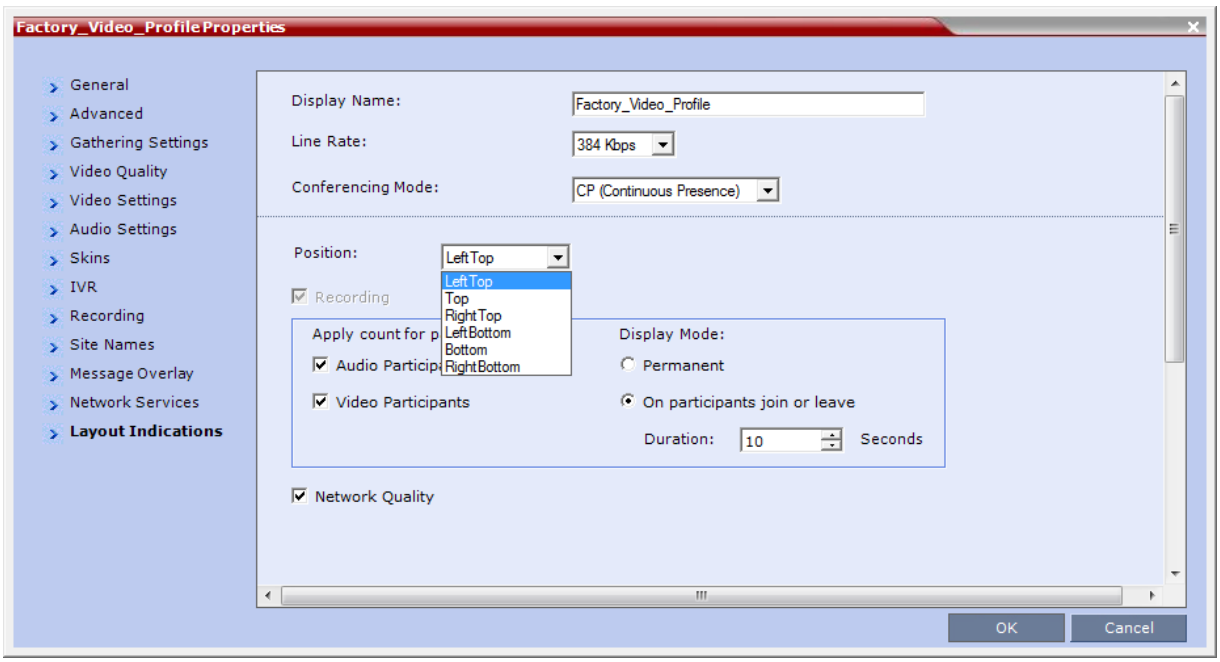
User Interface

Video participant(s) presence is indicated by an icon, and a number adjacent (to the right) reflecting 0 to 99 video participants, or if more, 99+. The icon indicating video participant presence is:

Video participants indication appearance is dependent on selecting the **Video Participant** check-box in the **Conference Profile Properties > Layout Indications** tab.

This indication may appear permanently, or upon an endpoint joining or disconnecting from the conference, for the specified duration, all depending on the Collaboration Server user configuration in that tab.

In addition the Collaboration Server user can determine the position of the indication, as shown below.

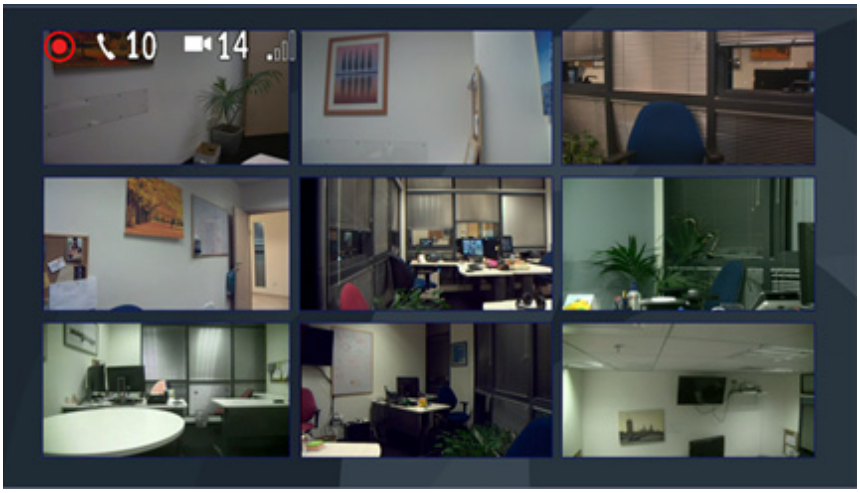


Order of Indications

The video participant is adjacent to the indications for recording, audio participants, and network quality. These indications are ordered from the outside, towards the inside, in the order:

- Recording indication
- Audio participant indication
- Video participant indication
- Network quality indication

Below, is an example of the layout indication order, when all indication types are selected.



Layout Indications Guidelines

- Layout indications appear only on the video display of AVC endpoints, and are applicable for CP Only and Mixed CP and AVC conferencing modes.
- Lync users can view layout indications provided the video sent to the Lync endpoint is transcoded. However, layout indications are not embedded in the video sent to the link towards the AV MCU, to preserve the Lync user experience.
- When indications are set to appear upon a change in connected participants, all selected indications appear together, even when the change occurred only in one type of participants.

  However, when the change occurs in participants whose type is unselected, no indications appear (assuming the indication display is not permanent).
- Layout indications are displayed only in endpoints with resolutions of CIF and up.
- Layout indications are not displayed during the gathering phase.
- Remote participants (that is, connected to a cascaded conference) are not included in the count, as well as the cascading link itself. Layout indications are displayed within each Collaboration Server participants independently, thus no layout indications are embedded in the video sent towards the cascading link.

  In that context, Lync endpoints connected via the AV MCU are included in the count, although other video participants connected to the AV MCU conference are not included.
- The **Layout Indications** tab is hidden in SVC, VSW, and TIP-enabled conferences.
- Layout indications can be set only in conference profiles, and not for ongoing conferences.
- The same indication display duration is applicable for all indications.
- For TelePresence endpoints:
  - The layout indications appear only on the main screen.
  - Only non-TIP endpoints can view the layout indications.
  - TelePresence rooms with three screens are considered as a single endpoint in the video endpoints count.

- Upgrade of endpoints from audio to video, or downgrade from video to audio, is reflected in the layout indications count.
- PSTN/H.323 audio participants calling the Collaboration Server Gateway profile, and dialing-out a VMR on the DMA via SIP/H.323, are counted as either an audio or a video endpoint, regardless of the Collaboration Server they are connected to.
- AVC endpoints connected to a CloudAXIS client, can view layout indications, depending on the conference profile configuration.

Change SVC License ratio to 1:5

All licensed SVC port resource ratios have be enhanced to 1: 5 (Standard ports : SVC ports) on following systems:

- RMX 1800 with one DSP card
- RMX 1800 with three DSP cards
- RMX 2000 with MPMRx-S/D media card
- RMX 4000 with MPMRx-S/D media card
- RealPresence Collaboration Server, Virtual Edition (Soft MCU)

Besides, SVC maximum capacities of following systems are enhanced. In the Soft MCU, the maximum SVC capacity numbers are changed in the a-la-carte licensing mode. For RPP licensing mode, the numbers remain the same.

This enhancement is applicable to Mixed CP and SVC, and SVC only conferences.

Note: Decoding in 1080 SVC Mixed Conferences
In 1080 SVC Mixed Conference, only 360p SVC is decoded.

SVC Maximum Capacities Enhancement for Appliance Edition Collaboration Server

The following tables describe the SVC maximum capacities enhancement in the Appliance Collaboration Servers.

Maximum SVC Capacity Enhancement in Non-mixed Conferences

Product Type	Single MPMRx-s		RMX 1800 with 1 DSP Card	
Version	**V8.5**	**V8.6**	**V8.5**	**V8.6**
720 SVC	90	150	105	175
1080 SVC	90	150	105	175

Maximum SVC Capacity Enhancement in Mixed Conferences

Product Type	Single MPMRx-s		RMX 1800 with 1 DSP Card	
Version	**V8.5**	**V8.6**	**V8.5**	**V8.6**
720 SVC	75	75	90	90
1080 SVC	75	75	90	90

SVC Maximum Capacities Enhancement for Virtual Edition Collaboration Server

The following tables describe the SVC maximum capacities enhancement in the RealPresence Collaboration Server, Virtual Edition, in the a-la-carte licensing mode.

Enhancement in a-la-carte Licensing Mode

Note: Tables Applicability
The tables below refer to the Dual Intel E5-2690 platform as an example.

Maximum SVC Capacities Enhancement in Non-Mixed Conferences with a-la-carte Licensing Mode

Cores Number	32 Cores		16 Cores		8 Cores	
Version	**V8.5**	**V8.6**	**V8.5**	**V8.6**	**V8.5**	**V8.6**
720 SVC	90	150	45	75	22	35
1080 SVC	90	150	45	75	22	35

Maximum SVC Capacities Enhancement in Mixed Conferences with a-la-carte Licensing Mode

Cores Number	32 Cores		16 Cores		8 Cores	
Version	**V8.5**	**V8.6**	**V8.5**	**V8.6**	**V8.5**	**V8.6**
720 SVC	90	150	45	75	22	35
1080 SVC	90	150	45	75	22	35

Configuration option to disable G.729

A new System Flag, **ENABLE_G729**, has been added.

Modifying its value to **NO** ensures that the G.729 codec is disabled, and G.711 is used instead. This is useful in calls where audio quality is affected by lower line rates.

Range: YES (default) / NO

To modify the System Flag value, the flag must be added to the System Configuration file. System Reset is not required after changing the flag's value. The modified flag setting will affect new calls.

For more information see Modifying System Flags.

Copyright and Trademark Information

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom 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.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

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.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the Polycom Support Center for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.