RELEASE NOTES Version 8.6.7 | Dec 2016 | 3725-74600-029C3

Polycom® RealPresence® Collaboration Server, Virtual Edition

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, Virtual Edition 8.6.7 Changed Features

RealPresence® Collaboration Server, Virtual Edition 8.6.4 Changed Features

RealPresence® Collaboration Server, Virtual Edition 8.6.2 Changed Features

RealPresence® Collaboration Server, Virtual Edition 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, Virtual Edition 8.6.7 Changed Features 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.

RealPresence® Collaboration Server, Virtual Edition 8.6.7 Changed Features

The following table lists the changed feature in Collaboration Server, Virtual Edition 8.6.7

Version 8.6.7 - Changed Features

Category	Feature Name	Description
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.

RealPresence® Collaboration Server, Virtual Edition 8.6.4 Changed Features

The following table lists the changed feature in Collaboration Server, Virtual Edition 8.6.4

Version 8.6.4 - Changed Features

Category	Feature Name	Description
Collaboration	Polycom® RealPresence Clariti™ Support	RealPresence Collaboration Server 1800/Virtual Edition will be enabled with full capacity in the RealPresence Clariti solution.

RealPresence® Collaboration Server, Virtual Edition 8.6.2 Changed Features

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

Version 8.6.2 - Changed Features

Category	Feature Name	Description
Codecs		
WebRTC	WebRTC solution and Microsoft solution integration	WebRTC and Microsoft users can dial-in to the same conference based on the integration.
Miscellaneous		
Certificate	New CSR guideline.	A few changes to existing CSR guidelines.

Version 8.6.2 - Changed Features

Category	Feature Name	Description
IVR	Suppress Operator's Entry Tone	A new system flag.
Rest API	SNMP	Support configuring SNMP through Rest API.
Recording	RealPresence Media Suite/Capture Server Dial-In RealPresence Collaboration Server through H.323	Support recording / playback for H.323 calls.

RealPresence® Collaboration Server, Virtual Edition 8.6 New Features

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

Version 8.6 - New Features

Category	Feature Name	Description
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.
Lync	Common Chairperson between Collaboration Server and AVMCU	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.
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.
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, via DNS.
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.
Endpoints and Codecs		

Version 8.6 - New Features

Category	Feature Name	Description
WebRTC	Modular MCU with WebRTC support, and WebRTC Service support.	WebRTC - VP8 and OPUS - in Mixed Group Browser Call. This allows Web endpoint participants in Collaboration Server conferences.
Audio	Configuration option to disable G.729.	A system flag allows disabling G.729 is favor of G.711, to enhance audio quality.
Network and System		
Network - System	VM MCU on Hyper-V.	Collaboration Server, Virtual Edition can be deployed over Microsoft Hyper-V environment, thus unite purchase and support under Microsoft.
System	Support Upgrade / Downgrade of Collaboration Server VE	Upgrade / downgrade of Collaboration Server, Virtual Edition is supported, instead of reinstalling the Collaboration Server from scratch.
System	Over CPU Protection	A mechanism for detecting CPU overuse is created, to improve system robustness in overload conditions.
Network	OpenSSL upgrade	Some fixes of OpenSSL issues.
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.
Cascade	Snatch content over cascade link.	Snatching content token is now possible is cascading scenarios in addition to that of single MCU.
Miscellaneous		
Conferencing	4x5 Layout.	A simple 4x5 grid layout is added.
Conferencing	Show number of video participants.	AVC participants view indication on existence and number of video participants, in addition to previous audio participants indication.
Licensing, SVC	Change SVC License ratio to 1:5.	SVC licensing ratio is enhanced.

Products Tested with this Release

The RealPresence Collaboration Server (RMX) 1800/2000/4000/Virtual Edition system is tested extensively with a wide rang 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.

Note: Supported Products

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.

Note: Mixing Virtual Environment

Polycom supports mixed Hyper-V/VMware environments, but Polycom has not tested all configurations/combinations.

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)

Device	MCU Type		
	2000/4000	1800	Virtual Edition
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
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			

Device	MCU Type		
	2000/4000	1800	Virtual Edition
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
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

Device	MCU Type		
	2000/4000	1800	Virtual Edition
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
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

Device	MCU Type		
	2000/4000	1800	Virtual Edition
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
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)

Device	MCU Type		
	2000/4000	1800	Virtual Edition
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
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, Virtual Edition systems to this release.

Virtual Edition Host Server Platform Profile

This section provides information on the minimal Virtual Machine host settings and configuration, required for the deployment of RealPresence Collaboration Server, Virtual Edition, of which some are manual.

Note: Dedicated VM Server

To maximize audio and video quality, Polycom strongly recommends a dedicated VM server per Collaboration Server.

The described configuration is not mandatory; however, failing to follow it may result in degraded video and audio performance. Due to differences between hardware and VM environments, the performance information below is provided for guidance purposes only, and does not represent a guarantee of any kind by Polycom.

Deployment Settings - Minimum / Recommended

Component	Minimum Deployment Settings	Recommended Deployment Settings
vCPU	25000 MHz Reservation	90000 MHz Reservation
Memory	16 GB Reservation	16 GB Reservation
Network Adapter (NIC)	2 x 1Gbit	2 x 1Gbit
Hard Disk (Thin/Thick Provisioning)	30 GB	30 GB
Performance	14 SD ports or 7 HD ports	60 SD ports or 30 HD ports

NOTE: vCPU

For Intel CPUs, when Hyperthreading is enabled, the numbers above refer to logical cores (vCores) and not physical ones.

Note: Network Interface Card

Depending on the environment, the virtual machine might need a Network Interface Card (NIC) from the host dedicated for the virtual machine. For more information, refer to your VMware administrator.

An example for a recommended deployment is a 32 logical cores machine at 2.9GHz.

To install a virtual MCU from scratch, 60GB is required.

CPU Reservations for Licenses Purchased

The Administrator is required to change the number of cores per socket so that the total number of cores reflects the CPU cores required for the purchased licenses.

The table below demonstrates the more common/likely machines. Other systems might require some experimentation.

Number of Cores Required for Licenses Purchased

Number of Licenses Purchased	CPU Configuration				
	Dual Intel E5-2690 32 cores	Dual Intel E5-2680 32 cores*	Dual Intel E5-2650 32 Cores*	Dual Intel E5-2620 24 Cores	Dual Intel X5660 24 Cores*
5 ports	5	5	7	8	8
10 ports	10	11	14	16	16
15 ports	16	17	21	24	24
20 ports	21	23	29	NA	NA
25 ports	26	29	NA	NA	NA
30 ports	32	NA	NA	NA	NA

* These numbers are estimates only, and may require adjustment.

NOTE: Hyperthreading

These numbers assume that hyperthreading is enabled in the physical server's BIOS. If hyperthreading is disabled, the above numbers are approximately halved.

NOTE: Over-allocation of Cores

Do not over-allocate cores.

For more information, refer to *RealPresence Collaboration Server, Virtual Edition, Getting Started Guide*.

Upgrade Package Contents

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

- RealPresence Collaboration Server, Virtual Edition documentation:
  - RealPresence Collaboration Server, Virtual Edition Version 8.6 Release Notes
  - Polycom RealPresence Collaboration Server, Virtual Edition, Getting Started Guide
  - Polycom RealPresence Collaboration Server, Virtual Edition, Administrator's Guide V8.6
- 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
  - Polycom XML Tracer User's Guide
  - XML Schemas
  - Polycom XML Tracer application

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. Perform the upgrade as documented for your system.

Upgrading from Version 8.5 to Version 8.6

The method of upgrading the Virtual Edition MCU is similar in look and feel to that of its hardware based counterparts.

In addition the MCU remains active during the upgrade, and can host conferences, until the reboot required to complete the upgrade procedure.

To upgrade the Virtual Edition MCU:

1. Backup the configuration file:

a Select **Administration > Software Management > Backup Configuration**.

b In the **Backup Configuration** window, click **Browse** to select a backup directory.

c Click **Backup** to back all configurations in the directory.

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

3 Browse to the Install Path, selecting the **.upg** file for upgrade, or **.ova** file for a complete installation, in the folder where Version 8.7 is saved, and click **Install**.

The installation of the upgrade proceeds. A progress bar is displayed while the files are copied and the software is installed.

When the installation completes, a dialog prompts the administrator to reset the MCU to complete the upgrade.

4 Reset the MCU, at your convenience, to complete the upgrade (until reset, the previous version is operational). For more information on Collaboration Server reset, see *RealPresence® Collaboration Server, Administrator Guide*, Administration and Utilities chapter.

Upgrading from a Version Earlier than 8.5 to Version 8.6

To upgrade the Virtual Edition MCU:

1 Backup the configuration file:

a Click **Administration > Software Management > Backup Configuration**.

b In the **Backup Configuration** window, click **Browse** to select a backup directory.

c Click **Backup** to back all configurations in the directory.

2 Download the VE V8.6 image from the Support Site:
http://support.polycom.com/PolycomService/support/us/support/network/collaboration_conferencing_platforms/realpresence_collaboration_server_ve.html

The file to download for upgrade has a .upg extension (the ova file is for installation from scratch).

3 Reboot the machine.

4 Create a New Virtual Instance of the VE.

For more information see the *RealPresence® Platform Director™ Administrator's Guide*:
http://supportdocs.polycom.com/PolycomService/support/global/documents/support/setup_maintenance/products/network/Platform_Director_ag_1_7_0_us.pdf

5 Restore the configuration file:

a Click **Administration > Software Management > Restore Configuration**.

b In the **Restore Configuration** window, click **Browse** to select the configuration file that was backed up

c Click **Restore**.

6 If the Collaboration Server is used with a RealPresence DMA system, enable the RealPresence DMA system functionality:

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

b Select **Network > MCU > MCUs**.

c Select the MCU and choose **Start Using**.

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

Upgrading from Version 8.3 to Version 8.6

During this procedure your Collaboration Server must be added to your RealPresence Platform Director Environment.

To upgrade the Virtual Edition MCU:

1 Install RealPresence® Platform Director™.

The RealPresence Platform Director is included with all Virtual Edition products and is available at the Polycom Support Site for download.

http://support.polycom.com/PolycomService/support/us/support/network/index.html

2 Upgrade your Collaboration Server using the same steps described in the Upgrading from Version 8.5 to Version 8.6 section above.

NOTE: Collaboration Server stops working

The Collaboration Server stops working at this point, and must be added to the RealPresence Platform Director Environment.

3 Open the Platform Director and add your RealPresence System Component (Collaboration Server) to your RealPresence Platform Director Environment as described in the *RealPresence® Platform Director™ Administrator's Guide:*
http://supportdocs.polycom.com/PolycomService/support/global/documents/support/setup_maintenance/products/network/Platform_Director_ag_1_7_0_us.pdf

Upgrading the RMX Manager Application

The RMX Manager application can be downloaded from one of the RMX systems installed in your site or from Polycom web site at http://www.polycom.com/support.

You are recommended to install the latest version of the RMX Manager (version 8.1 and higher are supported).

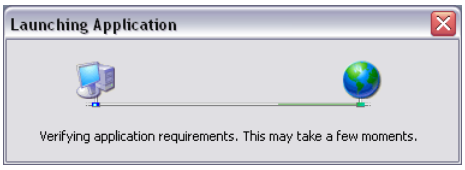
- When upgrading the RMX Manager application, it is recommended to backup the MCU list using the **Export RMX Manager Configuration** option. For more details, see *Polycom RealPresence Collaboration Server, Virtual Edition, Administrator's Guide*, *Software Management*.
- When upgrading the RMX Manager from a major version (for example, version 8.0) to a maintenance version of that version (for example, 8.0.1), the installation must be performed from the same MCU (IP address) from which the major version (for example, version 7.0) was installed.

  If you are upgrading from another MCU (different IP address), you must first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs**.

To install RMX Manager (downloading the application from the RMX):

1 Start Internet Explorer and connect to the RMX from which the current version was installed.
The Login screen is displayed.

2 Click the **Install RMX Manager** link on the upper right corner of the Login screen.
The installer verifies the application's requirements on the workstation.



If the following error message is displayed: "You cannot start application RMX Manager 7.8 from this location because it is already installed from a different location" you are upgrading from an MCU that is other than the one used for the installed version (different IP address).

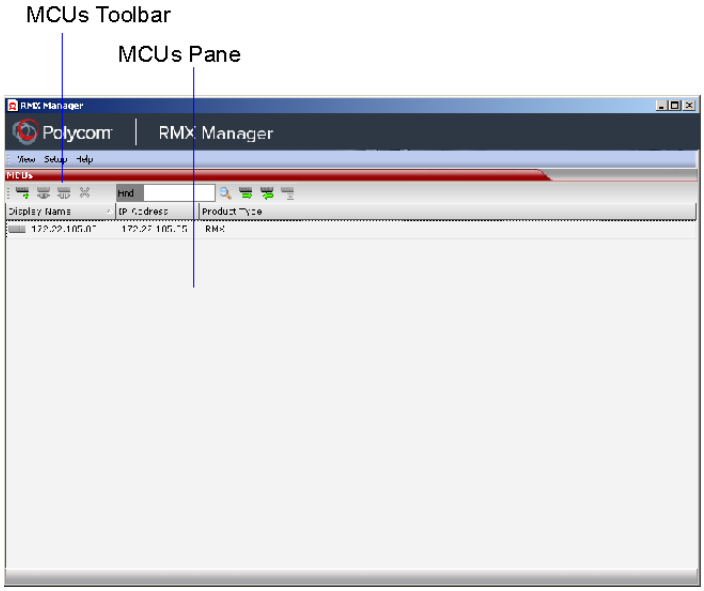
In such a case, first uninstall the RMX Manager application using **Control Panel > Add or Remove Programs**.

The **Install** dialog box is displayed.

3 Click **Install**.

The installation proceeds.

The installation completes, the application loads and the **MCUs** screen is displayed.



The list includes the previously defined MCUs.

If the MCUs list is empty, import the backed up list using the **Import RMX Manager Configuration** option. For more details, see *Polycom RealPresence Collaboration Server, Virtual Edition, Administrator's Guide* Import/Export RMX Manager Configuration.

For example, if the speaker's endpoints has two screens and the participant's endpoint only one, the participant's display is divided into two video layout cells with each video layout cell showing the input of one of the speaker's screens (endpoint).

If the participant endpoint has two screens, and the speaker endpoint only one, the speaker's video will be displayed on one of the participant's screens, while the second screen remains black.

Known Issues

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

Known Limitations

Issue ID	Category	Description	Detected in Version	Workaround
BRIDGE-23495	Content	In a 2 MB mixed CP and SVC conference and the content set to HiResGraphics with multiple content resolutions, the shared content is poor and illegible.	V8.6.3	
BRIDGE-22404	Content	Content shared is not received by the client if Enhanced Content Server is not used.	V8.6.3HF	
BRIDGE-23809	Content	When connected to VMR post through DX70/80, content sharing does not work.	V8.6.4	
BRIDGE-23526	Content	After implementing hold/resume the content on RealPresence Group Series, the content no longer displays on TelePresence SX10.	V8.6.4	
BRIDGE-23527	Content	After implementing hold/resume the content on Cisco Cisco EX90, the content no longer displays on RealPresence Group Series.	V8.6.4	
BRIDGE-23528	Content	After implementing hold/resume the content on Cisco TelePresence SX20, the content no longer displays on RealPresence Group Series.	V8.6.4	
BRIDGE-8132 / 19658/ 17293	Content	Content cannot be shared when dialing-out from a CP only conference with content set to H.263 & H.264 to Tandberg Edge95 (MXP) endpoints over H.323.	V8.2	
BRIDGE-19514	Content	Content received on RealPresence Mobile device stops when HDX endpoint joins the conference. HDX endpoint does not receive Content either.	V8.6	
BRIDGE-13342	Content	On Collaboration Server VE, Content is not seen on Cisco H.323 endpoints registered with CUCM when working in TIP Video + Content Mode.	V8.4	Use Prefer TIP 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-16806	General	Quality of Service (QoS) for SVC is enabled, but sometimes packets are unmarked.	V8.5	Fixed in 8.5.5 release
BRIDGE-1441	General	Automatic reboot fails after modifying system flags even though system prompts reset.	V7.8.0	

Known Limitations

Issue ID	Category	Description	Detected in Version	Workaround
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-22462	Interoperability	In a WebRTC conference, when a WebRTC client calls RealPresence Collaboration Server, Virtual Edition through Chrome 46.0.2490.86 running on MacOS 10.11.1, the count of the dropped packets does not always increase, sometimes the count number decreases.	V8.6.3	
BRIDGE-8393	Interoperability	A Cisco-registered HDX, connected as audio-only to an RMX conference, running at 256kpbs on a Cisco Unified Communications Manager, automatically disconnects from the conference.	V8.2	
BRIDGE-3929	Interoperability	If the SoftMCU is registered to a Siemens Server using TCP, after reseting the SoftMCU the SoftMCU will display the system alert, “Failed to connect to SIP registrar.”	V8.1.2	
BRIDGE-22	Interoperability	In a 768 kbps conference with 1 H.323 endpoint and 2 SIP endpoints, one of which was a M100, when the M100 disconnected it still showed as connected on the MCU.	V7.8.0	
BRIDGE-18739	Interoperability	Collaboration Server fails to dynamically adjust media quality (resolution and frame rate) to changes in bandwidth/bitrate for WebRTC endpoints, resulting in possible reduction in video/audio quality, or at times, disconnection of WebRTC endpoints.	V8.6	In conference involving WebRTC endpoints, configure lower line rate in either Conference Template in DMA (impacts all conferences using this template), or in RPWS (RealPresence Web Suite) Experience Portal for WebRTC bridge calls (impacts all WebRTC endpoints).

Known Limitations

Issue ID	Category	Description	Detected in Version	Workaround
BRIDGE-18423	Interoperability	In a conference with a line rate of 1920kbps with external SVC and internal and external AVC endpoints, audio and video freezes on all endpoints when speaking from external SVC endpoint.	V8.4.5	
BRIDGE-15236 / 17122 / 19849	Interoperability	At times, Collaboration Server VE connects Cisco endpoints over H.323 to a 4M CP conference, with these endpoints connected as "connected with problem"	V8.5	
BRIDGE-1333	Interoperability	On a Collaboration Server VE, after a second SIP RPD audio only endpoints joins, only one Audio Rx is shows is listed in RPD statics when there should be two.	V7.8.0	
BRIDGE-10808	Interoperability	When an HDX 8000 registered to a SIP server connected to an MCU registered to a DMA 7000 attempt to connect to a mixed AVC-SVC 1920 kbps conference using a line rate of 64 kbps, instead of connecting as audio only the connection failed.	V8.3, V8.3.1	
BRIDGE-19465 / 19519	Interoperability	PC and Macintosh clients using Chrome 42 with IPv6 enabled, have difficulties connecting to WebRTC conferences when DMA selects an IPv6 ICE candidate address.	V8.6	During ongoing conferences, retry connecting. Before conference creation, disable IPv6 on PC and Macintosh clients.
BRIDGE-2340	IP	Failure to remove first IP address on a list of NT server addresses.	V8.0	
BRIDGE-6587 / 19637/ 17039	IVR	In the IVR Service after rebooting a Collaboration Server VE, the “enable welcome message” check box becomes unchecked and the welcome audio message is not played.	V8.1.7	
BRIDGE-13892	Licensing	Collaboration Server VE is activated with maximum licensed ports instead of the reservation actually made in the FNE server.	V8.4	
BRIDGE-16323 / 16746 / 16747	MPM Card	The maximum number of SVC participants per conference a single MPMRx card may handle is limited to 5 (60 conferences*5 participants).	V8.5	

Known Limitations

Issue ID	Category	Description	Detected in Version	Workaround
BRIDGE-19560 / 20114	Partners - Microsoft	Failed to RealConnect a Polycom endpoint to a conference on the AVMCU, using the organization prefix associated with the CAA of that organization, and the conference ID.	V8.6	
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-86	SIP	In an SVC dial-in conference with 8 endpoints using SIP over UDP some endpoints may not update the layout in bad network connections.	V7.8.0	Use SIP over TCP instead of UDP.
BRIDGE-8004/ 19660/ 17295	SIP	SIP endpoints may intermittently disconnect after a conference has run for more than 30 minutes.	V8.2	
BRIDGE-19518	SIP	Conference on Collaboration Server VE with 13 WebRTC clients as participants, was terminated, due to 7 out of 13 endpoints receiving erroneous transaction ID from the DMA in the SIP UPDATE request.	V8.6	
BRIDGE-993	SVC	During a conference started from a Profile, after an SVC RPD participant dials-in, the Participants Properties - SDP tab, Remote Capabilities pane lists no information.	V7.8.0	
BRIDGE-23815	Video	WebRTC Dynamic Bandwidth Adaption does not work properly. In a MCU-bridged WebRTC conference with 512 Kbps line rate, WebRTC clients do not receive VGA video, instead they receive video with 352x240 resolution.	V8.6.4	
BRIDGE-23472	Video	Rarely when RealPresence Group Series, HDX, RealPresence Desktop, RealPresence Mobile and RealPresence WebSuite endpoints dial into MCU-bridged WebRTC conference simultaneously, slow motion video layouts display on RealPresence WebSuite endpoint.	V8.6.4	

Known Limitations

Issue ID	Category	Description	Detected in Version	Workaround
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	
BRIDGE-7307	Video	In a conference with 1 OTX and 2 TPX's with the OTX and 1 TPX connecting using ITP conference room switching, after applying MLA automatic layout, a black bar is displayed on the central monitor of the OTX.	V8.1	
BRIDGE-14489	Video	Slightly different color of video cell borders and the space between the video cells in the lower left skin example of the Profile, on Collaboration Server, Virtual Edition, when selecting a skin with background.	V8.5	
BRIDGE-10140	Video	VSX receives no video in SIP call registered to DMA.	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, Virtual Edition.

Issue ID	Category	Description
BRIDGE-24764	Gateway	While in VEQ, a Segmentation Fault in ConfParty process occurs and core dump is created.
BRIDGE-24629	Interoperability	IDEA and RC4 Cipher Suite are present in Client Hello for RMX 1800 and SoftMCU EDGE platform.
BRIDGE-24557	Interoperability	In DMA system VMR conferences, several endpoints are disconnected from the conference at the same time.
BRIDGE-24426	Software Version	After upgrading RealPresence Collaboration Server, Virtual Edition to version 8.6.3.29, all calls failed with the major alarm “Media is Recovering”
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.

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, Virtual Edition.

Issue ID	Category	Description
BRIDGE-23460	Content	When a Web Suite participant shares and stops content, all other participants see frozen content on their screens.
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-23532	General	Dynamic Bandwidth Adaption does not work properly after RealPresence Collaboration Server, Virtual Edition upgrade.
BRIDGE-22966	General	RealPresence Collaboration Server, Virtual Edition fills its root filesystem fast until a reboot.
BRIDGE-22702	General	RealPresence Collaboration Server, Virtual Edition uses too much disk space, and the free space keeps decreasing. Major alarm reporting the remaining free disk space displays in Fault list.

BRIDGE-22648	General	When a user displays the Click & View menu and disconnects, the next caller to connect sees the Click & View menu when using RMX Virtual Edition MCU.
BRIDGE-22523	General	Duration doesnot display correctly as configured for Meeting Room.
BRIDGE-22716	General	Collaboration Server 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-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-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-23226	Interoperability	Call speed and resolution mismatch between RealPresence Desktop and VSW high profile of RealPresence Collaboration Server.
BRIDGE-22544	IVR	Participants' endpoints do not forward the "Invite Participant" DTMF code in ISDN calls on RMX Appliance and Virtual MCUs.
BRIDGE-23603	Partners - Microsoft	VMR Lync calls are disconnected due to ICE check failure.
BRIDGE-23335	Partners - Microsoft	In the RealConnect conference, no audio can be heard by Lync participants, and bad audio is heard by the RealPresence Collaboration Server, Virtual Edition participants. Video is fine.
BRIDGE-23367	Partners - Microsoft	RealConnect call fails to connect to RMX 1800 until reboot RMX 1800. CSS Gateway disconnection, AVMCU disconnection or DNS error occurs in such failures.
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.

Issues Resolved in Version 8.6.3

The following table lists the issues resolved in the 8.6.3 release of the RealPresence® Collaboration Server, Virtual Edition.

Issue ID	Category	Description
BRIDGE-22869	Interoperability	Call fails when WebRTC client uses Chrome version 48.0 and RealPresence Collaboration Server, Virtual Edition version is 8.6.3.6.
BRIDGE-20916/ 21476	Interoperability	WebRTC calls to a bridge fail with Chrome 45 (Canary), and users receive a "You have been disconnected from the meeting" message.

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, Virtual Edition.

Issue ID	Category	Description
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-19438	General	After upgrade and restore the backup on RealPresence Collaboration Server, Virtual Edition, Address Book is not accessible and becomes empty.
BRIDGE-19296	General	Call flow timing issue causes call drops in the active conference on Collaboration Server.
BRIDGE-20396	General	PARTY_IDENT_INFO is added in Visual Name.
BRIDGE-20166	Interoperability	MCCF error is reported on Collaboration Server in the process of DMAs Failover and primary DMA service recovery.
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-19352	IP	On RealPresence Collaboration Server, Virtual Edition, when setting DHCP to off through console, error message displays, but actually the DHCP mode is turned off successfully.
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, Virtual Edition.

Issue ID	Category	Description
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-16438	Partners - Microsoft	Video on Lync 2013 clients using Collaboration Server VE freezes in calls to a VMR when a third endpoint joins the VMR.
BRIDGE-14090 / 16415 / 16473	Partners - Microsoft	Video from the Collaboration Server freezes when a virtual meeting room (VMR) is cascaded with Lync Server 2013, and Lync 2010 clients are participants in the call.
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.

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, Virtual Edition

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

Contents

Version 8.6.7 Virtual Edition Detailed Description of Changed Features

Version 8.6.4 Virtual Edition Detailed Description of Changed Features

Version 8.6.2 Virtual Edition Detailed Description of Changed Features

Version 8.6 Virtual Edition Detailed Description of New Features

Copyright and Trademark Information

Version 8.6.7 Virtual Edition Detailed Description of Changed Features

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 Virtual Edition Detailed Description of Changed Features

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 Virtual Edition Detailed Description of Changed Features

WebRTC Feature

Change to existing WebRTC feature in version 8.6.2 is:

- WebRTC and Microsoft Deployments Integration

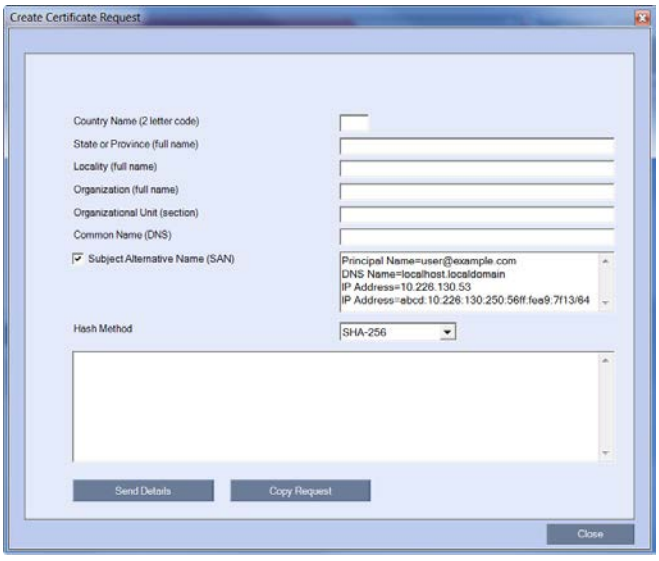
Miscellaneous Features

Changes to existing miscellaneous features in version 8.6.2 are:

- 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 Virtual Edition 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 s Service Provider.

The features in that category are:

- New RealConnect Topology for Service Provider
- Common Chairperson in Collaboration Server and AVMCU
- Reestablishing Connection to AVMCU via DMA 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

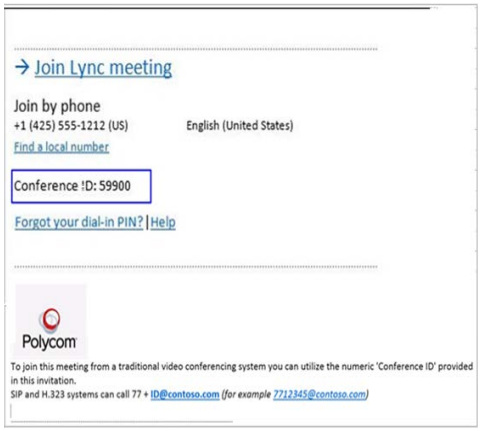
As part of supporting video conferencing in a Polycom-Lync environment, Polycom supplies Polycom® ContentConnect® for Microsoft Lync environments (previously known as Content Sharing Suite, or CSS), which enables content sharing between Lync and non-Lync conference participants.

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.



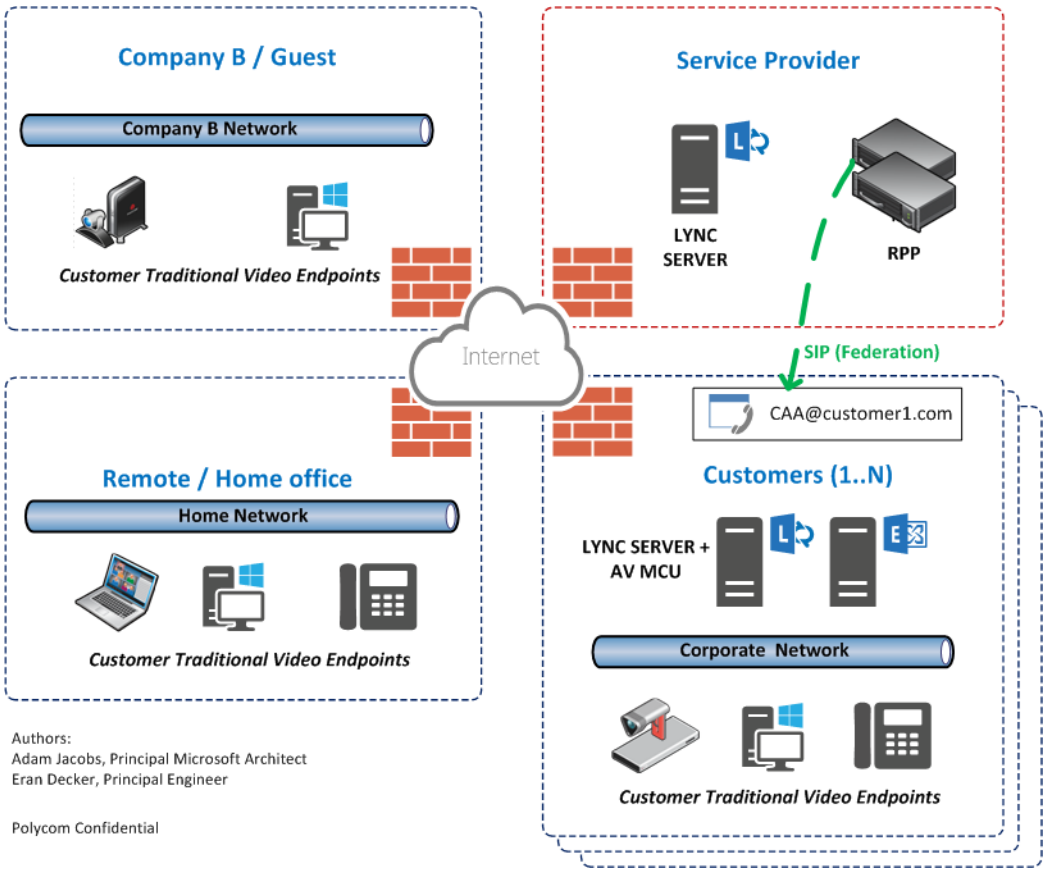
- The RealConnect connection is established within 7 seconds, at the most.
- The audio/video of non-Lync participants is muted/suspended during the process, so as to keep the RealConnect process hidden.

  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

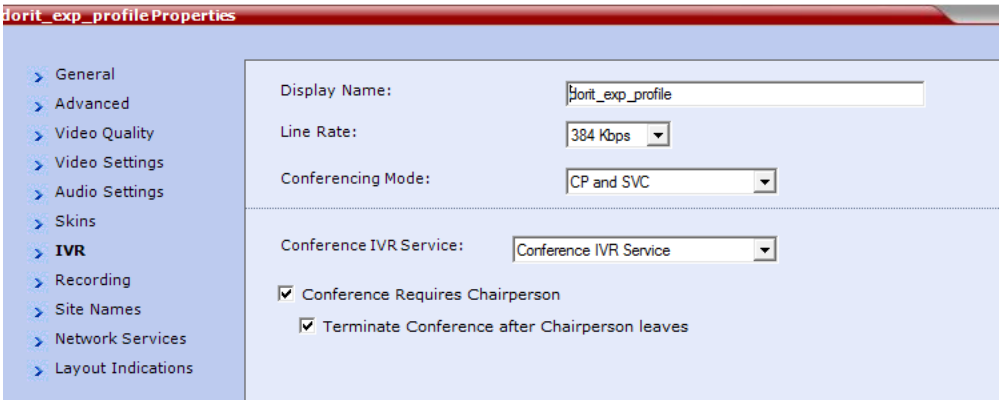
- If the federated organization prefix entry in the DMA table yields an erroneous CAA URI, the participant is immediately disconnected.
- If a non-Lync endpoint dials an erroneous number as the conference ID on the AV MCU, the participant is immediately disconnected.

Common Chairperson in Collaboration Server and AVMCU

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 to AVMCU via DMA 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.

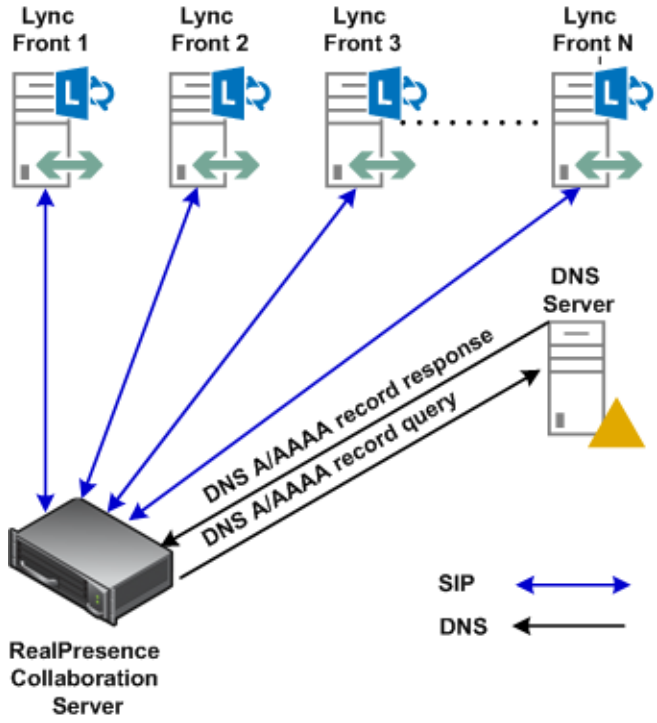
DNS Load Balancing on Lync Front End Pool

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.

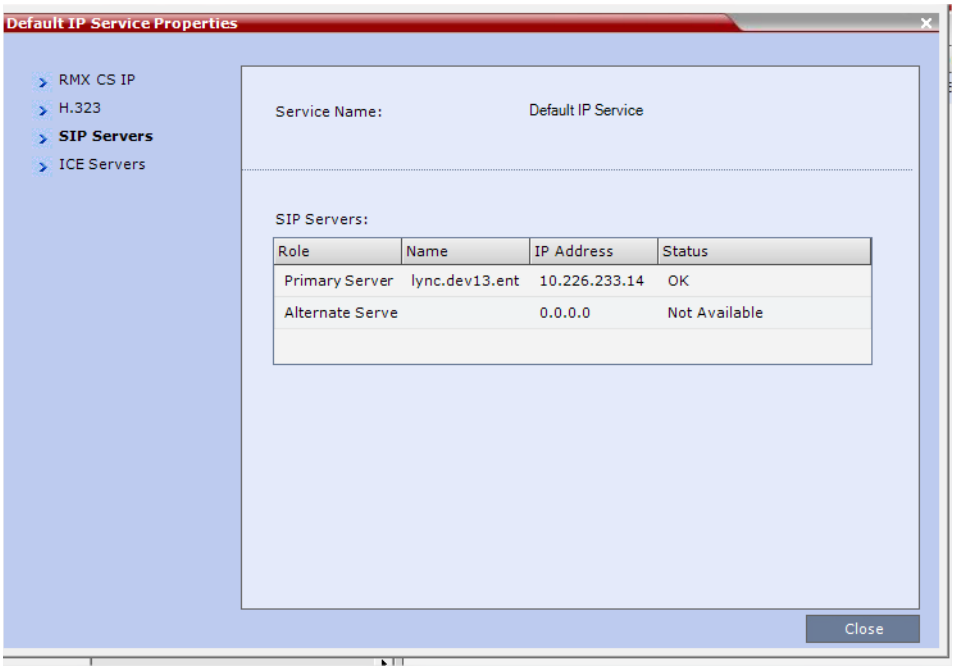


All Front End (FE) servers in the pool register themselves in DNS server with the same FQDN but different IP addresses (both IPv4 and IPv6 are supported).

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.

Endpoint and Codec Features

The central Network features in the V8.6 release are WebRTC support.

These features include:

- WebRTC and WebRTC Service Support
- Configuration option to disable G.729

WebRTC and WebRTC Service Support

Note: WebRTC / Web Suite Disclaimer
WebRTC video conferencing requires RealPresence Web Suite with a RealPresence Web Suite Pro license. Do not enable any WebRTC features unless your video conferencing environment includes RealPresence Web Suite Pro. For complete documentation, please see the *RealPresence Web Suite Administrator Guide*.

Polycom Web Real-Time Communication (WebRTC) Solution Overview

Polycom WebRTC solution requires following components:

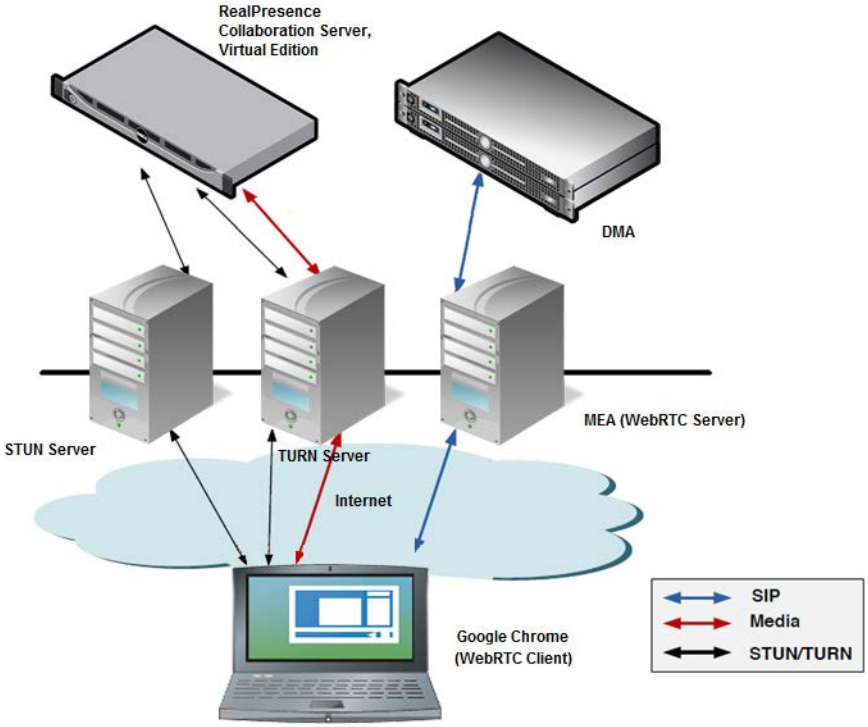
WebRTC Solution Required Components

Solution Component	Role and Main Function
Polycom® RealPresence® Collaboration Server, Virtual Edition	Media transcoding and hosting the bridged conference
Polycom® RealPresence® Distributed Media Application, Virtual Edition	Load balancing and SIP server, the WebRTC solution license.
Polycom® RealPresence® Access Director	STUN/TURN server for firewall traversal
Polycom® RealPresence® Web Suite Pro	WebRTC server as web portal and signaling gateway
Google Chrome	Web browser on WebRTC client
Polycom® ContentConnect™	Content sharing

WebRTC solution also supports optional components, for more information refer to *Polycom RealPresence Web Suite Administrator Guide* at:

http://support.polycom.com/PolycomService/support/us/support/network/cloudaxis_suite/realpresence_web_suite.html

The following graphic shows an example with required components for a WebRTC bridged conference deployment.



WebRTC Bridged Conference

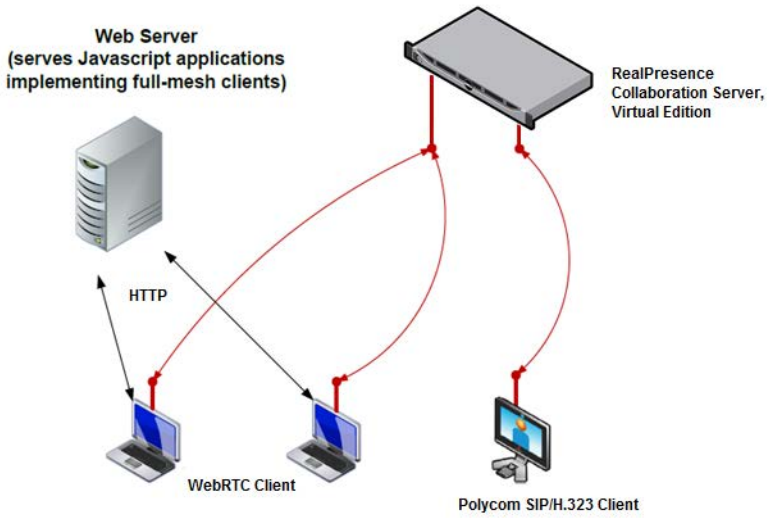
A bridged conference can be either:

- An original bridged conference
- An original mesh conference is transited to a bridged conference

For more information refer to *Polycom RealPresence Web Suite Administrator Guide* at:

http://support.polycom.com/PolycomService/support/us/support/network/cloudaxis_suite/realpresence_web_suite.html

The following graphic shows how a WebRTC client and a Polycom client join the bridged conference. In the conference, the Collaboration Server, Virtual Edition implements the transcoding, for example, between VP8 and existing video protocols.



Supported Features in WebRTC Bridged Conference

The following features are supported on RealPresence Collaboration Server, Virtual Edition in a bridged conference:

- VP8 video and Opus audio transcoding
- ICE (STUN and TURN) support
- DTLS / SRTP support
- RTP / RTCP support including
  - Video and audio bundling
  - Multiplexing/demultiplexing RTP channels
  - RTCP Feedback (RTCP-FB) message
  - Status report: Sender Report (RR)/ Received Report (SR)
- SDP Support

WebRTC and Microsoft Deployments Integration

RealPresence Collaboration Server, Virtual Edition, supports WebRTC and Microsoft deployment integration, through which Polycom clients Lync/Skype for Business (SfB) clients, WebRTC clients, and their legacy clients can be connected to the same conference.

To integrate WebRTC and Microsoft deployments into one, two scenarios are available as described:

- RealPresence Collaboration Server Hosted Conference

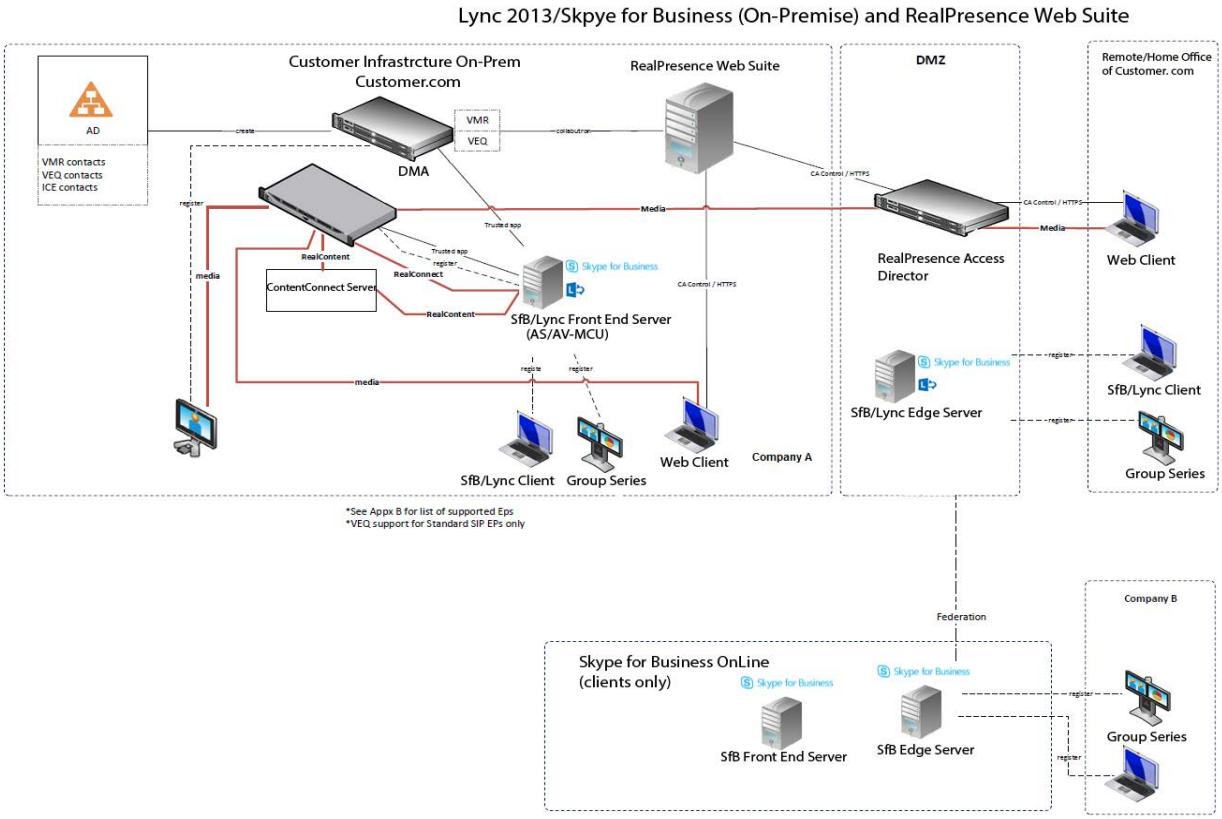
  Microsoft Lync/SfB clients and Polycom standard video clients connect directly to a conference hosted on the RealPresence Collaboration Server. WebRTC clients connect to the same conference through RealPresence Access Director.

- RealConnect Cascaded Conferences through predefined VMR

  Lync/SfB clients connect to a conference on the SfB/Lync 2013 FE Server (AS/AV MCU) while Polycom standard video clients connect to a separate conference on the RealPresence Collaboration Server. WebRTC clients that reside outside or within the enterprise connect through RealPresence Access Director to the conference on the RealPresence Collaboration Server.

  The conference on RealPresence Collaboration Server is cascaded to the conference on AS/AV MCU through a VMR predefined on DMA, thus all clients join the same cascaded conferences with a unique, predefined VMR.

The following shows an example of Lync 2013/Skype for Business On-Premise deployment integration with WebRTC deployment.



- Lync 2013/SfB On-Premise: The RealPresence Collaboration Server joins a Trusted Application Relationship with the SfB/Lync FE Server (AS/AV MCU). Polycom and WebRTC clients connect to RealPresence Collaboration Server conference which cascades to AV MCU conference. That results in one cascaded conference where Polycom, WebRTC and Lync/SfB clients can see and hear each others. With a ContentConnect server deployed, all clients can share content in the conference. All Network elements of Lync 2013/SfB On-Premise deployment are located at Company A.
- SfB On-line clients at Company B or Home Office/Remote site are connected to SfB/Lync Edge server in DMZ.
- WebRTC clients at Home Office/Remote site are connected to RealPresence Collaboration Server at Site A through RealPresence Access Director in DMZ.

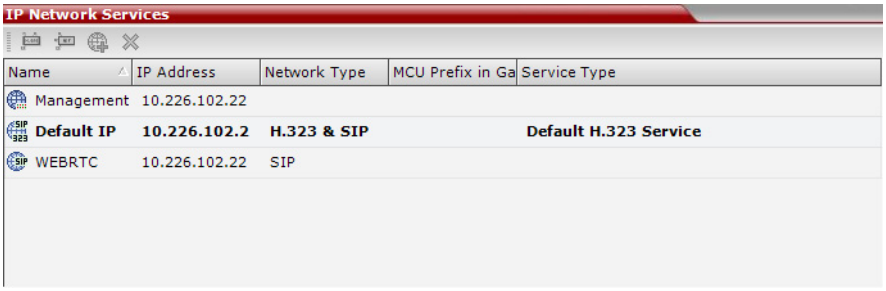
In both of the scenarios, all clients can hear and see each others, and with a ContentConnect server deployed, all clients can share and receive content in the conference. WebRTC clients can receive the roster of the conference in the RPP (but not including the Lync clients), but WebRTC clients cannot dial into a Lync Outlook scheduled conference.

Currently, dialing into the RealConnect conferences through a Outlook invitation is not supported in the WebRTC and Microsoft deployments integration.

Two IP Network Services for Generic/Microsoft and WebRTC

The RealPresence Collaboration Server, Virtual Edition, supports configuring up to two IP Network services:

- First mandatory IP Network service is used for either a generic or a Microsoft service.
- Second optional IP Network service is used for the WebRTC service.The WebRTC service is configured through RealPresence Collaboration Server, Virtual Edition, but all WebRTC functions are processed on a modular MCU.



Microsoft/Generic Network Service Configuration

- Generic Network Service Configuration

  For Generic Network service configurations, refer to the IP Network Services section in *RealPresence Collaboration Server, Virtual Edition Administrator Guide*.

- Microsoft Network Service Configuration

  1. Open the IP Network Service dialog, and in the **IP** tab, select **IP Network Type** to **SIP**.
  2. Install a Security Certificate in the **SIP Servers** tab of the IP Network Services Properties dialog box:
     - **a** In the **Certificate Method** drop-down menu, select **PEM/PFX**.
     - **b** Click the **Send Certificate** button.
     - **c** Browse to the saved Certificate on the Workstation and click the **Yes** button to install the certificate.
  3. Register to Lync Server:
     - **a** In the **SIP Server** field, select Specify.
     - **b** In the **SIP Server Type** field, select **Microsoft**.
     - **c** Set **Refresh Registration** to every **3600** seconds.
     - **d** If not selected by default, change the Transport Type to **TLS**.
     - **e** In the **SIP Servers** table, enter the IP address of the Lync Server in both the **Server IP Address or Name** and **Server Domain Name** fields.
     - **f** In the **SIP Servers** table, the **Port** field must be set to **5061**.

g In the **Outbound Proxy Servers** table, enter the IP address in the **Server IP Address** or **Name field**. (The same value as entered in Step f.)

h In the Outbound Proxy Servers table, the Port field must be set to 5061 (the same value as entered in Step g).

For more information see the *Polycom Unified Communications Deployment Guide for Microsoft Environments*.

WebRTC Network Service Configuration

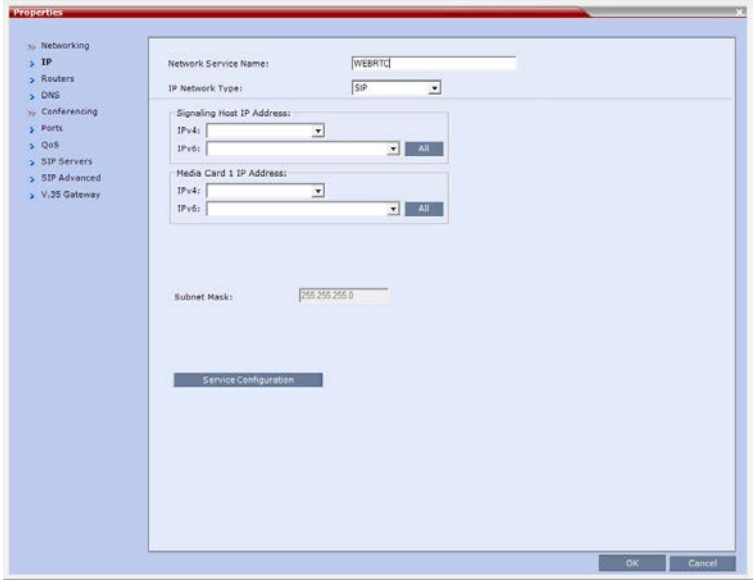
Some configurations once configured on Microsoft/Generic IP Network Service will be applied to WebRTC IP Network Service. These configurations includes:

- Network
- IP
- Routers
- DNS
- Security

To configure the WebRTC Network Service:

1. In the **RMX Management** pane, select **IP Network Services**.
2. Click **New IP Service** ( ).

   The service **IP** dialog box is displayed.



WebRTC Properties – IP

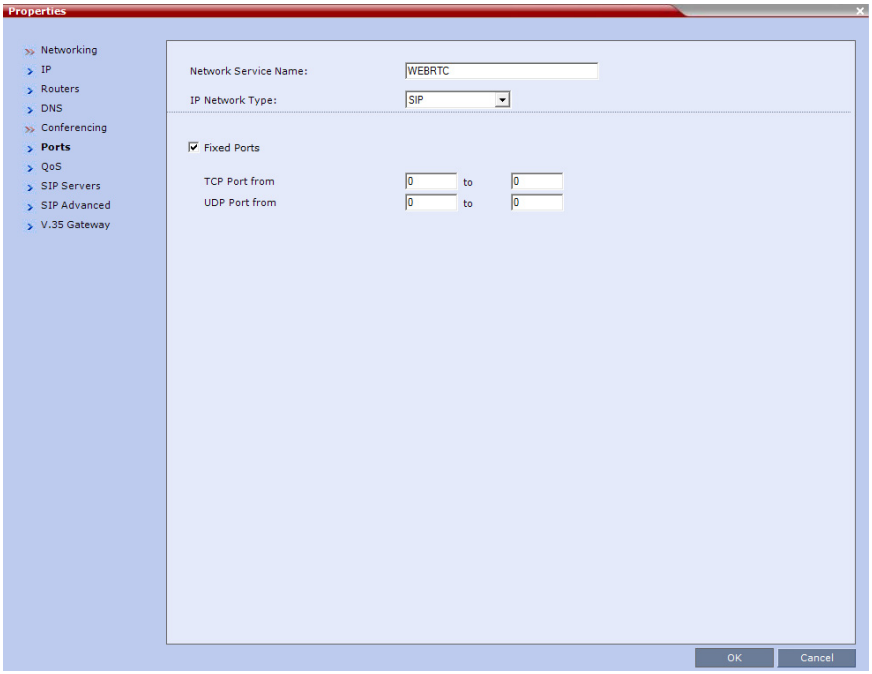
Field	Specification
Network Service Name	Specifies the name for the IP Network service.
IP Network Type	Specifies the IP Network type to **SIP** for WebRTC Network Service.

WebRTC Properties – IP

Field	Specification
Signaling Host IP Address	
IPv4	Selects the signaling host IPv4 address from the drop-down list.
IPv6	This is auto filled once the signaling host IPv4 address has been specified.
Media Card 1 IP Address	
IPv4	Selects the media card 1 IPv4 address from the drop-down list.
IPv6	This is auto filled once the media card 1 IPv4 address has been specified.
Subnet Mask	Displays the subnet mask.
Service Configuration	Clicks the button to open the System Flags dialogue box.

3 Select the **Ports** tab.

The **Ports** dialogue box is displayed.



WebRTC Properties – Ports

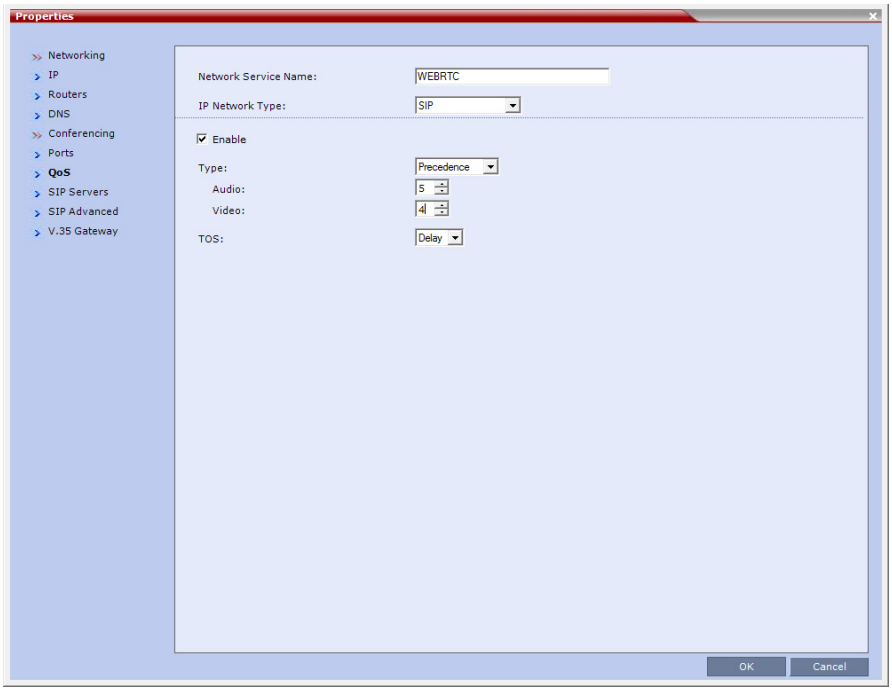
Field	Specification
Network Service Name	Changes the specified name for the IP Network service if needed.
IP Network Type	Changes the IP Network type that has been specified if needed.

WebRTC Properties – Ports

Field	Specification
Fixed Ports	Selects to enable TCP or UDP port configurations.
TCP Port Type	Specifies the number range of the TCP ports.
UDP Port Type	Specifies the number range of the UDP ports.

4 Select the **QoS** tab.

The **QoS** dialogue box opens.

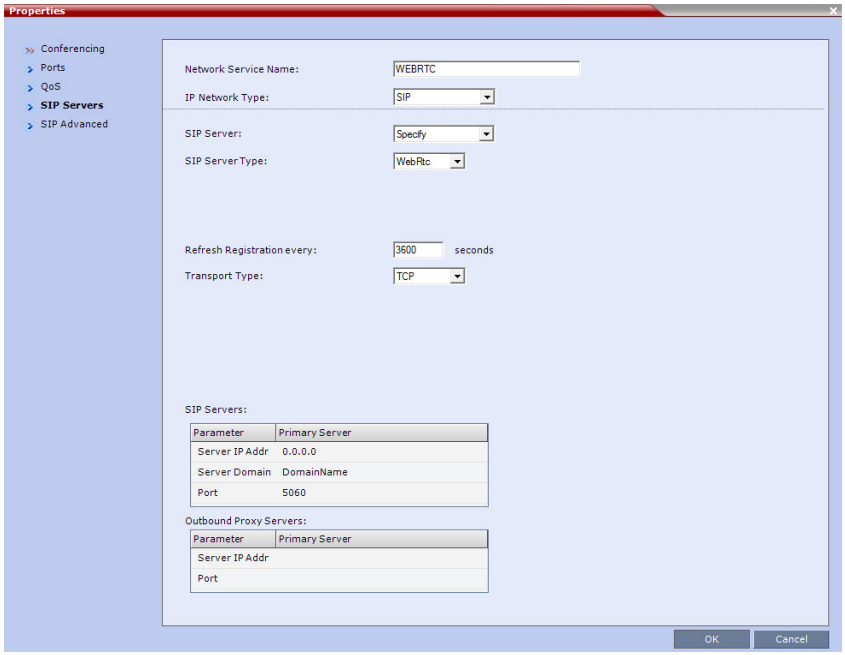


WebRTC Properties – QoS

Field	Specification
Network Service Name	Changes the specified name for the IP Network service if needed.
IP Network Type	Changes the IP Network type that has been specified, if needed.
Enable	Selects it to enable QoS configurations for WebRTC service.
Type	Specifies the Diffserv or Precedence as the WebRTC QoS type. If Precedence is selected, you can specify the Precedence for WebRTC Audio or Video respectively, both of the value ranges are from 0 to 5.
TOS	TOS can be configured only if Precedence is selected. You can specify whether transmit WebRTC service as normal or with delay.

5 Select the **SIP Servers** tab.

The **SIP Servers** dialogue box is displayed.



WebRTC Properties – SIP Servers

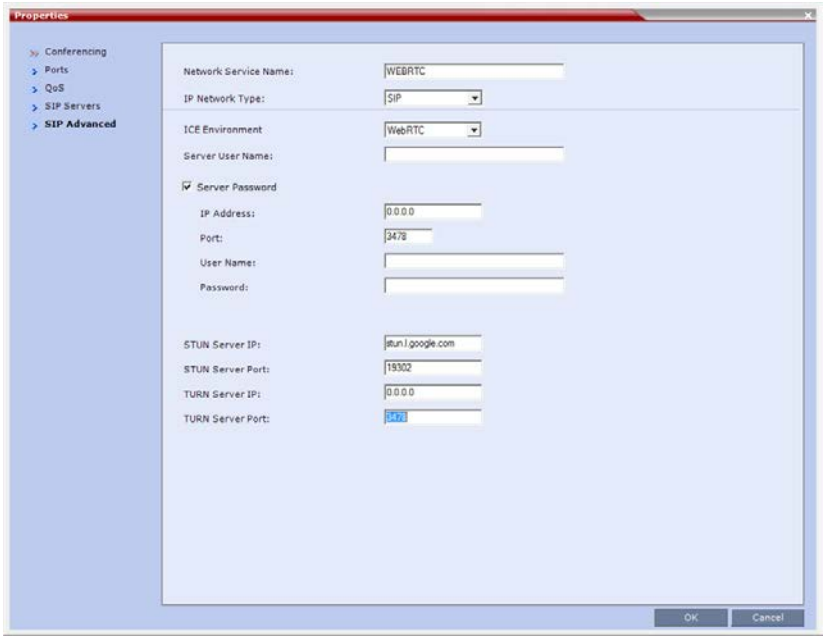
Field	Specification
Network Service Name	Changes the specified name for the IP Network service if needed.
IP Network Type	Changes the IP Network type that has been specified, if needed.
SIP Server	Specifies the SIP Server to **Specify** in the drop-down list.
SIP Server Type	Specifies the SIP server type to **WebRtc** in the drop-down list.
Refresh Registration every	Specifies the time period that RealPresence Collaboration Server, Virtual Edition refreshes the registration in SIP server.
Transport Type	Displays the transport type. **Note**: The transport port type can be TCP, UDP or TLS, the transport port type is synchronized from the first configured IP Network service.
SIP Servers	
Server IP address	Displays the SIP server IP address.
Server Domain	Displays the SIP sever domain.
Port	Displays the SIP server port.
Outbound Proxy Servers	

WebRTC Properties – SIP Servers

Field	Specification
Server IP address	Displays the proxy server IP address.
Port	Displays the proxy server port.

6 Select the **SIP Advanced** tab.

7 The **SIP Advanced** dialogue box is displayed.



WebRTC Properties – SIP Servers

Field	Specification
Network Service Name	Changes the specified name for the IP Network service if needed.
IP Network Type	Changes the IP Network type that has been specified if needed.
ICE Environment	Specifies the ICE environment to WebRTC.
Server User Name	Specifies the SIP server user name.
Server Password	Select the check box to enable SIP server configurations.
IP address	Specifies the SIP server IP address.
Port	Specifies the SIP server port.
User Name	Specifies the SIP server user name.
Password	Specifies the SIP server password.
STUN Server IP	Specifies the STUN server IP address.
STUN Server Port	Specifies the STUN server port.
(Optional) TURN Server IP	Specifies the TURN server IP address.
(Optional) TURN Server Port	Specifies the TURN server port.

The following table shows the relationship between SIP configurations and ICE environment configuration.

Relationship between SIP configurations and ICE environment.

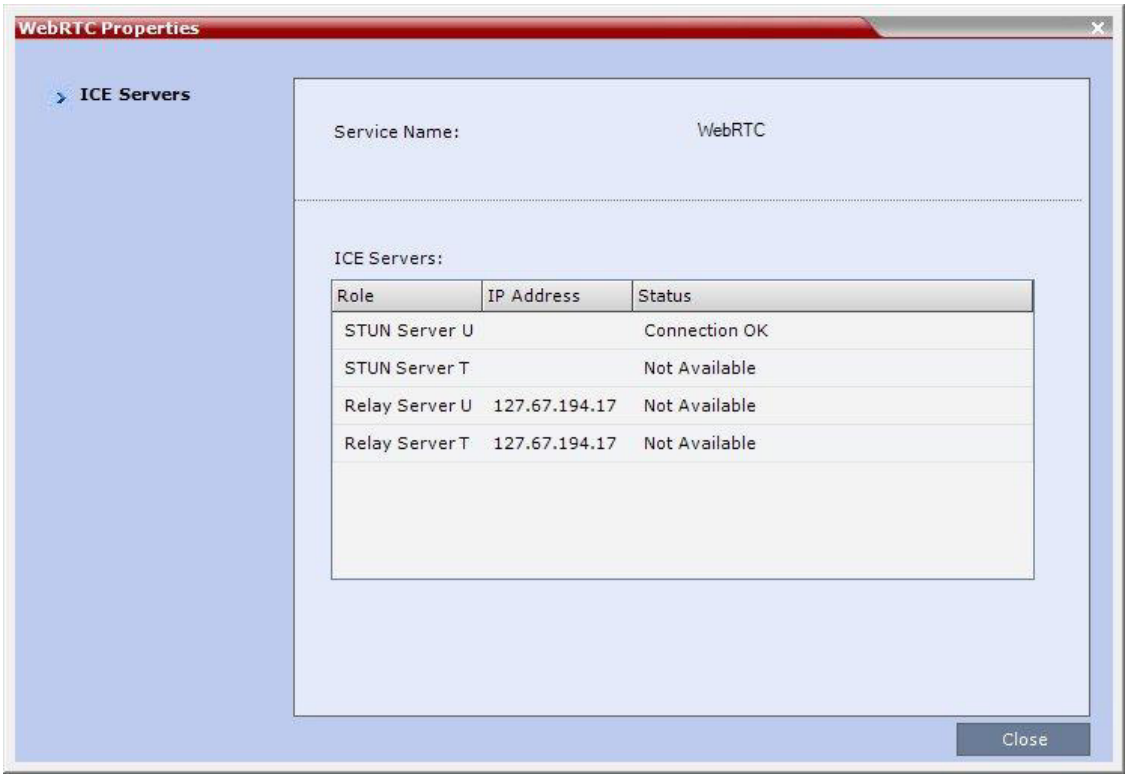
SIP Server Configuration	SIP Server Type Configuration	Allowed ICE Environment configuration
Off	NA	None/Standard/Microsoft
Specify	Generic	None/Standard
	Microsoft	None/Microsoft
	WebRtc	None/WebRTC

After configuring both the Microsoft IP Network Service and the WebRTC IP Network Service, you need to create a Lync VMR on DMA and then all clients can connect to the conference through the unique VMR.

For how to join from WebRTC client, refer to *Polycom® RealPresence® Web Suite User Guide*.

WebRTC Service Monitoring

You can monitor the WebRTC connection through **RMX Management** > **Signaling Monitor**.



Conference Features Supported on WebRTC/Non-WebRTC Clients

A dual E5-2690 CPU on the Collaboration Server can currently provide WebRTC clients with a maximum of 30 WebRTC VGA/SD ports or 20 HD720p30 ports using VP8 as video Codec and Opus as audio Codec respectively. You can check the media information, including the video protocol, resolution and frame rate, through **Participant Properties** > **Channel Status - Advanced** tab.

The following table indicates the conference features applicable to WebRTC and Non-WebRTC clients.

Conference Features Applicable to WebRTC/Non-WebRTC Client

Feature	Non-WebRTC Client	WebRTC Client
Dial In	Yes	Yes
Dial Out	Yes	Yes
Audio-only Calls	Yes	Yes
Roll Call	Yes	Yes
Exit/Entry Tones	Yes	Yes
Site Names	Yes	Yes
Speaker Indication	Yes	Yes
Lecture Mode	Yes	Yes

Conference Features Applicable to WebRTC/Non-WebRTC Client

Feature	Non-WebRTC Client	WebRTC Client
DTMF	Yes	Yes, only if web browser has supported DTMF implementation as RFC 4733 defined.
PCM and Click&View	Yes	Yes, only through out-of-band DTMF as RFC 4733 defined.
Message to participants/Message Overlay	Yes	Yes
Indications on Layout	Yes	Yes
Gathering Phase	Yes	Yes
IVR	Yes	Yes
Operator Conference	Yes	Yes
Content Sharing with CSS	Yes	Yes
FECC	Yes	• WebRTC endpoint cannot control other cameras on other endpoints. • Cameras of WebRTC endpoints are not controlled by other endpoints.
Mute/Unmute	Yes	Yes
Hold/Resume	Yes	No
Conference Recording	Yes	Yes
ITP/TIP Support	Yes	Yes
CDR	Yes	Yes

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.

Network and System Features

The central Network and system feature in the V8.6 release is Hyper-V as the virtual platform for Collaboration Server VE.

The Network features are:

- VM MCU on Hyper-V
- High CPU Usage Detection
- Support for Skype for BusinessOpenSSL Upgrade

VM MCU on Hyper-V

Hyper-V is the hypervisor-based virtualization role of Windows Server.

Collaboration Server, Virtual Edition Deployment Methods

Collaboration Server, Virtual Edition can be deployed through **.vhd* files on Hyper-V in any of following methods:

- Deploy on Windows Server 2012 R2
- Deploy on Hyper-V Server 2012 R2
- Deploy using Virtual Machine Manager (VMM) of System Center 2012 R2

It is recommended to deploy the Collaboration Server, Virtual Edition on Windows Server 2012 R2.

Collaboration Server, Virtual Edition Licensing

The Collaboration Server, should then be licensed via the Platform Director version 1.7.1 or higher.

- View licenses availability
- Allocate licenses
- Deallocate licenses
- View license allocations/usage

For more information, refer to the *RealPresence Platform Director System Administrator's Guide*.

In a conferencing solution deployment, VMware and Hyper-V can be used simultaneously for different virtual edition products.

Support Up/Downgrade of Collaboration Server Virtual Edition

Beginning with this version, the method of upgrading the Virtual Edition MCU will be similar in look and feel to that of its hardware based counterparts.

The new method eliminates:

- The necessity to update the system's serial number.
- The installation of new certificates.

In addition the MCU remains active during the upgrade able to host conferences until the reboot that is required to complete the upgrade procedure.

To upgrade the Virtual Edition MCU:

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

2 Browse to the Install Path, selecting the **.upg** file for upgrade, or **.ova** file for a complete installation, in the folder where Version 8.6 is saved and click **Install**.

   The installation of the upgrade proceeds. A progress bar is displayed while the files are copied and the software is installed.

   When the installation completes a dialog prompts the administrator to reset the MCU to complete the upgrade.

3 Reset the MCU, at your convenience, to complete the upgrade (until reset, the previous version is operational). For more information see the *RealPresence® Collaboration Server, Virtual Edition Getting Started Guide*, Resetting the RealPresence Collaboration Server Virtual Edition.

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

The cascade related features are:

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

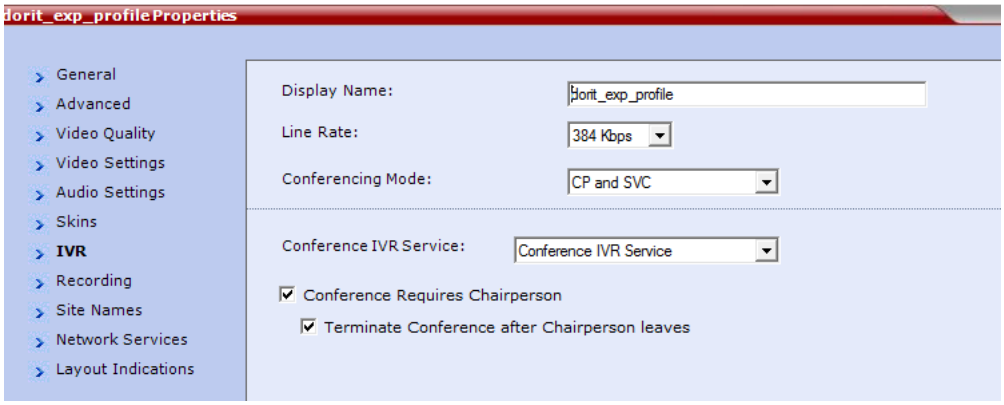
Enable Chairperson Managing Cascaded Meetings

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 an H.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.

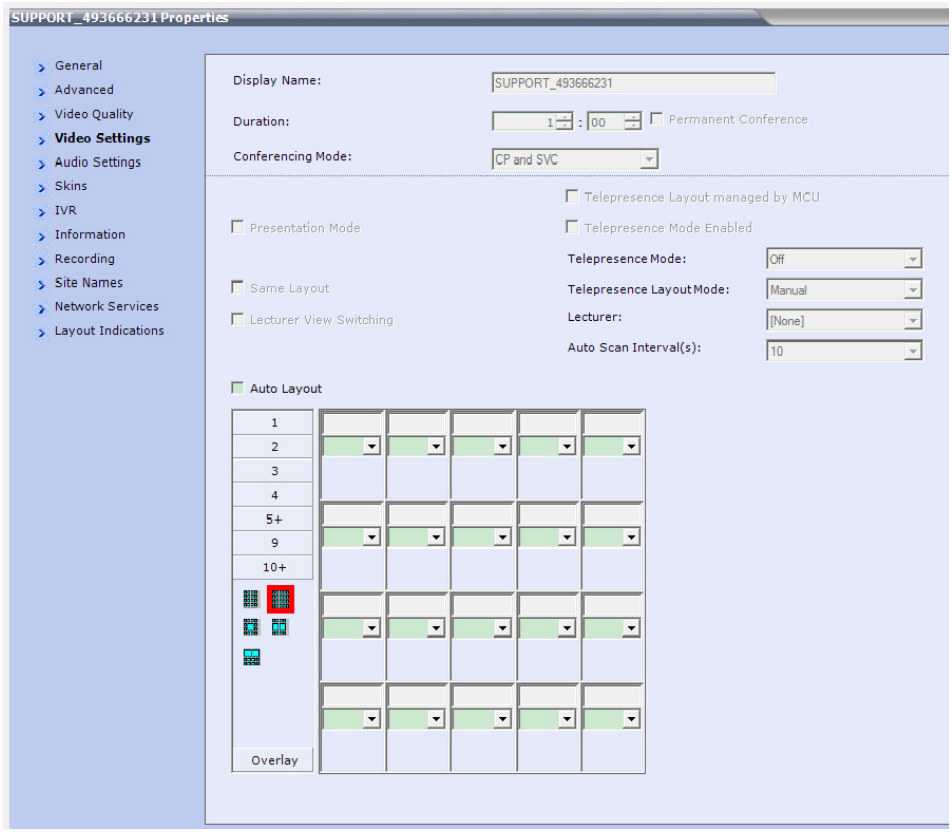
Miscellaneous Features

General features in version 8.6 are:

- New 4x5 Layout
- Video Participants Indication
- Change SVC License ratio to 1:5

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.

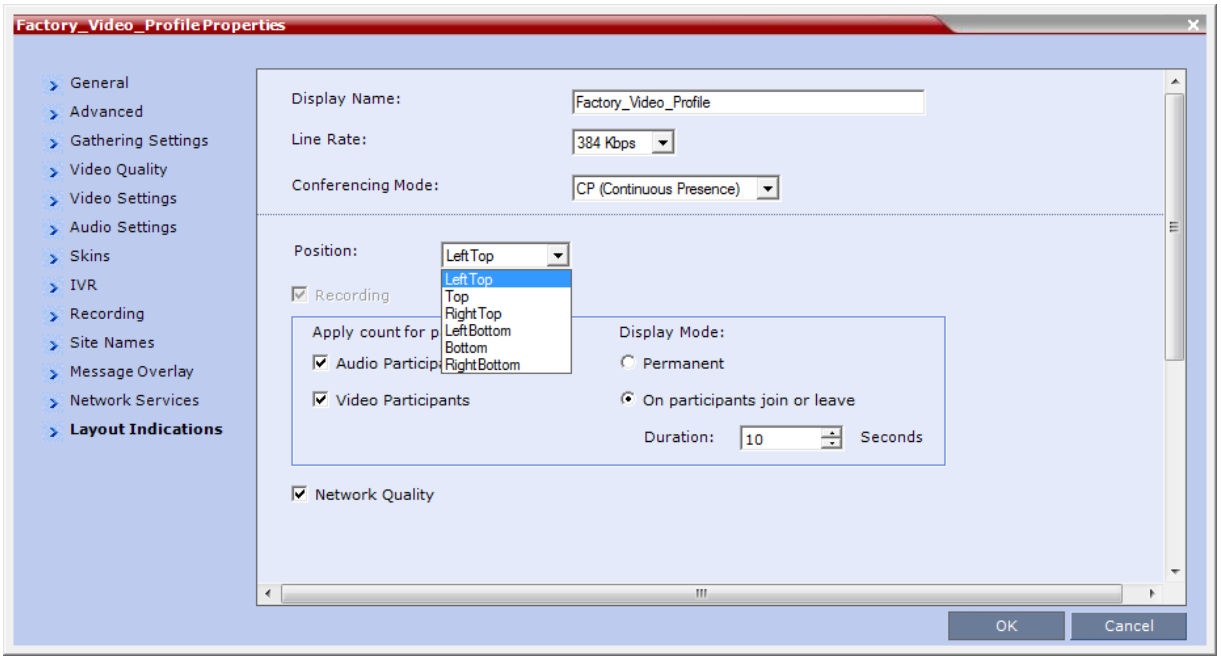
User Interface

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.

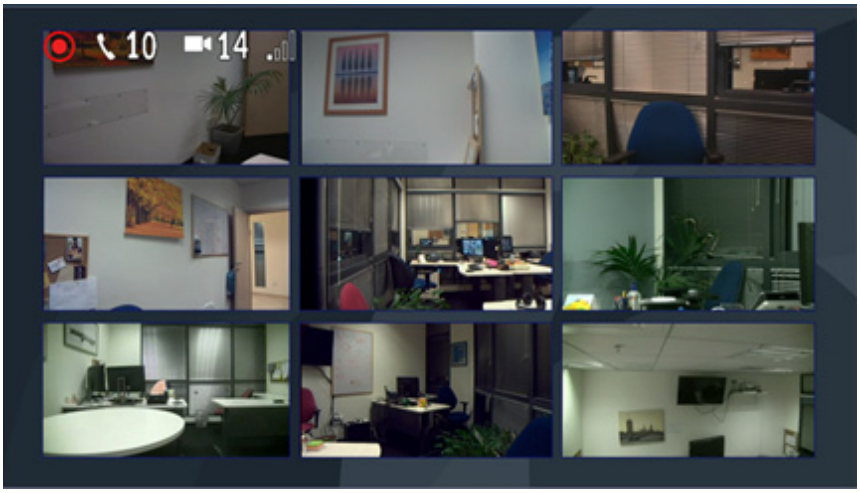


Order of Indications

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

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.