Cisco TelePresence MCU 4.3(2.30)

Software Maintenance Release Notes July 2012

Contents

Product documentation

The following documents provide guidance on installation, initial configuration, and operation of the product:

- Cisco TelePresence MCU 4200 Series Getting started
- Cisco TelePresence MCU 4500 Series Getting started
- Cisco TelePresence MCU MSE 8420 Getting started
- Cisco TelePresence MCU MSE 8510 Getting started
- Cisco TelePresence MCU 4.3 Product administration guide
- Cisco TelePresence Call Detail Records File format reference guide
- Cisco TelePresence MCU API 2.9 reference guide
- Cisco TelePresence Accessing Conferences Getting started guide MCU 4.3

New features in version 4.3

Version 4.3(2.30) is a maintenance release of software version 4.3 for the following Cisco TelePresence MCU products:

- Cisco TelePresence MCU 4200 Series
- Cisco TelePresence MCU 4500 Series

- Cisco TelePresence MCU 4501 Series
- Cisco TelePresence MCU MSE 8420
- Cisco TelePresence MCU MSE 8510

The products are generically referred to as ‘the MCU’ in this document.

This document lists and describes the new features introduced by the point release 4.3(1.68), and issues resolved by subsequent maintenance releases.

In call menus

Version 4.3 includes the ability to control many aspects of a conference while participants are on a call without needing to access the web interface. These are controlled using menus accessed via the control keypad. Pressing * on the keypad activates the in call menus.

The in call menus can be made available to chairs only, or to both chairs and guest participants, or disabled completely. Chairs can be configured to have access to the in call menus at one of three command levels:

Level 1
Local commands - request floor, mute/unmute audio and video, change layout, view participants.

Level 2
Level 1 commands plus **Conference** commands - assign floor to a participant, mute/unmute audio or video of participants, lock the conference, disconnect all participants, change a participant’s volume, send DTMF tones to a participant, disconnect a participant.

Level 3
Levels 1 and 2 plus **Advanced** commands - add participant, add/change PIN/guest PIN.

Guests can be given access to Local commands only.

To configure access to in call menus, go to the **Participant controls** section of the conference’s configuration page - click **Conferences,** click the conference to be configured then click the **Configuration** tab. Set the *In call menu for chair* and *In call menu for guests* parameters as required.

Note that in call menus are not currently supported over cascade links.

A user guide to the in call menu is incorporated in Cisco TelePresence Accessing Conferences Getting started guide MCU 4.3.

Hybrid and passthrough content

In previous versions, the MCU decoded all content video such as presentations, and encoded a single new stream to send out to all participants within a conference. In Version 4.3, the MCU can be configured to pass through a content stream without decoding and encoding it. This can reduce latency and increase quality, and does not require a video port on the MCU.

Sending a single video stream to everyone in a conference, whether encoded or passed through, can result in a single participant reducing the quality for everyone. If one participant can only receive SD video while everyone else can receive HD, then everyone receives SD video. This means that everyone receives a lower resolution than if only HD participants had been present.

Hybrid mode helps avoid this issue. In hybrid mode the incoming content stream is passed through, giving the best possible quality. It is also decoded and used to create a second, lower resolution stream for anyone who cannot receive the passthrough stream. This uses up a video port but ensures that users get the advantages of both transcoding and passthrough.

In addition, in previous releases the codec used for content had to be setup manually, to either H.263+ or H.264. This can now be set to automatically choose the codec so that as many people as possible in the conference receive content video.

To enable these settings go to the **Content** section of the conference’s configuration page (**Conferences** then click on the conference to be configured).

Faster audio switching

Improvements to the audio mixing capabilities in Version 4.3 of the MCU enable it to prepare the outgoing stream more quickly than in previous versions. Any delay that occurs when the active speaker changes is reduced and participants will experience a more natural flow of conversation.

This function is enabled automatically and does not require configuration.

API improvements

Version 4.3 includes extensions to the MCU's API in order to allow greater automated control of units. New commands include:

- Ability to set and read all IP configuration settings
- Ability to set and read all H.323 and SIP registration settings
- Ability to set and read all unit-wide content, encryption and time settings
- The device.query message now indicates if the MCU is in a shutdown state
- The participant.statistics message now includes all information from the **Participant > Statistics** page

Cisco Unified Communications Manager (CUCM) integration

Version 4.3 includes improved integration with Cisco Unified Communications Manager (CUCM). This includes:

- Ability to receive Keypad Markup Language (KPML) messages for keypad control
- Improved identification of participant names
- Support for more authentication methods

These improvements to CUCM integration are applied automatically and do not require configuration.

Static ARP

In Version 4.3 it is now possible to statically configure associations between MAC addresses and IP addresses rather than being retrieved automatically from the network. This increases security for important units with a known MAC and IP address within the network.

To add static ARP entries, use the 'arp' command from the serial port command prompt.

Cisco rebranding

The Cisco TelePresence MCU is now rebranded as Cisco across its user interface, in order to provide clarity and consistency across the product range.

H.225 keepalives

In Version 4.3, the MCU sends periodic TCP keepalive messages on the call signaling connection of H.323 calls. This prevents firewalls from terminating the connection due to inactivity on the signaling channel.

The TCP keep-alive messages are sent automatically and this behavior does not require configuration.

SIP outbound

SIP outbound is a new way for the MCU to connect to SIP registrars that support this functionality. It means that instead of opening a new connection each time the MCU needs to communicate with the registrar, a single connection is established and used for all future communication. This improves security and helps with firewall traversal.

SIP outbound is used automatically and does not require configuration.

DNS SRV failover for SIP

In Version 4.3, if multiple SRV records are returned for a given hostname on a SIP DNS lookup, then if the first entry fails to respond the MCU will try the other entries in the list. This is especially used for SIP registrars, and provides redundancy in cases where there is an issue with the first registrar location.

DNS SRV failover is used automatically and does not require configuration.

Cisco TelePresence MCU MSE 8510 nHD media port mode

Version 4.3 includes a new media port mode, nHD mode, which transmits and receives video at up to w360p resolution. The advantage of this mode is that a single port license enables two nHD ports; so on a blade with 40 port licenses you could have 10 Full HD ports, 20 HD ports, 40 SD ports, or 80 nHD ports. This provides a cost effective way of having large conferences, especially in mass deployments where lower resolutions are regularly used.

To use nHD mode go to **Settings > Media ports** and select *nHD mode* from the *Media port mode* drop-down. A restart is required for the MCU to start using this mode.

Cisco TelePresence MCU MSE 8510 HD port capacity improvements

The capacity of Cisco TelePresence MCU MSE 8510 blades in Full HD mode has been increased in Version 4.3. In Version 4.3 Cisco TelePresence MCU MSE 8510 blades support 15 Full HD video participants, and 15 audio-only participants. Note that you will require 60 port licenses to use 15 Full HD ports.

The table below summarizes the port capacities of each of the MCU models in Version 4.3. Changes between Version 4.2 and Version 4.3 are shown in bold.

Model	Mode	Licenses per port	Video ports	Audio-only ports	Streaming and content ports
MCU 4203			6	6	6
MCU 4205			12	12	0
MCU 4210			20	20	0
MCU 4215			30	30	0
MCU 4220			40	40	0
MCU 4501	SD		12*	12*	6*
	HD		6*	6*	6*
	HD+		3[‡]	6*	0
	Full HD		3*	6*	0
MCU 4505	HD		12	12	12
	HD+		6[†]	12	0
	Full HD		6	12	0
MCU 4510	HD		20	20	20
	HD+		10[†]	20	0

Model	Mode	Licenses per port	Video ports	Audio-only ports	Streaming and content ports
	Full HD		10	20	0
MCU 4515	HD		30	30	30
	HD+		15†	30	0
	Full HD		15	30	0
MCU 4520	HD		40	40	40
	HD+		20†	40	0
	Full HD		20	40	0
MCU MSE 8420		1	40	40	0
MCU MSE 8510	**nHD**	**0.5**	**80**	**0**	**0**
	SD	1	80	0	0
	HD	2	20	20	20
	HD+	4	20	20	0
	Full HD	4	**15**	**15**	0

* Can be doubled using the MCU 6 to 12 HD port upgrade feature key.

† Can be doubled using the 1080p capacity upgrade feature key.

‡ Can be doubled using the MCU 6 to 12 HD port upgrade feature key. Can be quadrupled using both the MCU 6 to 12 HD port upgrade feature key and the 1080p capacity upgrade feature key.

Resolved issues

The following issues were found in previous releases and have been resolved in 4.3(2.30).

Resolved since 4.3(2.18)

Identifier	Description
CSCub05295	In previous releases, the MCU could experience an unexpected restart by not validating parameters read from an invalid H.264 bit-stream. This is resolved in this release.
CSCua15725	In previous releases, in rare circumstances, the MCU could restart when a participant was entering DTMF tones, followed by * or #, on the pin entry screen of a full conference. This is resolved in this release.
CSCua55120	In previous releases, the MCU could unexpectedly restart when a participant's main video, after having been stopped, was used as a content source. This is resolved in this release.
CSCtx00682	In previous releases, the MCU will incorrectly redirect an HTTP multicast streaming request from QuickTime streaming client to HTTPS. This is resolved in this release.
CSCtz03695	In previous releases, the MCU could experience an unexpected restart when writing a very long message to the Audit log. This is resolved in this release.
CSCtx77792	In previous releases, the MCU could experience an unexpected restart if it tried to allocate a socket for an incorrectly set up address family for a streaming or SIP/H.323 participant. This is resolved in

Identifier	Description
	this release.
CSCty61469	In previous releases, the MCU will only send a CIF resolutions to a Polycom RMX MCU even when the Polycom MCU is capable of receiving higher resolutions. This is resolved in this release.
CSCty67022	In previous releases, the MCU could get into a state when no streaming media can be played from the streaming page. This is resolved in this release.
CSCty83602	In previous releases, when using the MCU in HD mode, any configuration changes on the Settings page would render 'Video Receive Bit Rate Optimisation' and 'Flow Control On Video Errors' options unchecked and greyed out. This is resolved in this this release.
CSCty91132	In previous 4.3 releases, the display name field of a SIP participant was not always prioritised over the username of the participant. This is resolved in this release.
CSCtz35468	In previous releases, long term use of the Microsoft Internet Explorer web browser could result in the MCU gradually running out of memory, which could cause an unexpected restart.
CSCtz25884	In previous releases, the MCU could experience an unexpected restart if a participant creating a conference through the auto attendant was moved prematurely to the same conference via the web interface before completing the task of configuring the pin for that conference. This is resolved in this release.
CSCtz69665	In previous releases, the 'purge selected' button to delete selected conferences on the MCU did not work for certain localisation packages (e.g. Russian). This is resolved in this release.
CSCua09848	In previous 4.3 releases, the MCU API did not trigger an update through participant.enumerate when the active speaker in the conference changed. This is resolved in this release.

Resolved since 4.3(1.68)

Identifier	Description
CSCtz09450	In the previous 4.3 release it was possible to configure a cluster of four Cisco TelePresence MCU MSE 8510 blades in the Cisco TelePresence MSE 8000 chassis when we only officially support three blades. This is resolved in this release.
CSCtz03995	Previous versions of MCU software, running on platforms other than the MCU 5300, do not support cascading with the MCU 5300. This has been resolved in 4.3(2.18) on MCU platforms in general (this release), and in 4.3(2.17) on the MCU 5300 (first full release).
CSCty98522	In previous releases, when the display name override field was used for preconfigured participants, the MCU would only display that name on the video display but not on the web interface. This is resolved in this release. Note that if a non-printing character, e.g. a space, is used for the display name override, the web interface reverts to the participant's name instead of the non-printing override, but the video display still shows the override.
CSCtx48168	In previous releases, the MCU participant.enumerate API response would sometimes omit the 'callDirection' parameter. This has been resolved in this release.
CSCtx62208	In previous releases, if a conference template name ended with a space, it was not possible to edit any fields for that template. This has been resolved in this release.
CSCty06858	In previous releases, the MCU 4500 experienced an unexpected restart when the MCU tried to access a decoder that is not present or invalid. This has been resolved in this release.
CSCty07111	In previous releases, an MCU running in HD mode only sent CIF resolution to Polycom RSS2000 (v.4), even though Polycom can support resolutions up to 1080p at 30 frames per second. This has been resolved in this release.
CSCty10645	In previous 4.3 releases, the top menu bar was not rendered correctly on the Conferences ->

Identifier	Description
	Template page of the MCU web user-interface when a localization package was uploaded on the MCU. This has been resolved in this release.
CSCty13904	In previous 4.3 releases, when a localization package was uploaded on the MCU web interface, some of the fields were not displayed correctly. This has been resolved in this release.
CSCty22375	In previous releases, when a participant.remove API command was sent immediately after a participant.disconnect API command, the MCU would not successfully remove the participant from the participant list. This has been resolved in this release.

Resolved since 4.2(1.50)

Identifier	Description
CSCtt19422	In previous releases, when a SIP session was refreshed, the session version parameter in the MCU's SDP was not updated correctly. This caused an interoperability issue with IMS phone switch where the calls from MCU would disconnect. This is resolved in this release.
CSCtx76766	In previous releases, MCU could under certain circumstances experience slow performance when uploading large CDR logs (>100,000 messages) to TMS. This is resolved in this release.
CSCty98518	In previous releases, when a 2 Mbps SIP call was placed from an MCU in HD mode, the MCU participants page would incorrectly report the receive bandwidth as 4 Mbps instead of 2 Mbps. This is resolved in this release.
CSCtq91175	In previous releases, participants added to a conference via the API would not inherit the default layout control value of the conference. This has been resolved in this release.
CSCtq99800	In previous releases, the MCU did not attempt to register to the alternate gatekeeper if the primary gatekeeper had sent a URQ. This has been resolved in this release.
CSCtr15071	In previous releases, if a Cisco Unified Border Element (CUBE) was in the call path between the MCU and an endpoint, H.239 content negotiation was not possible. This has been resolved in this release.
CSCtr51282	In previous releases, under some circumstances a Polycom MGC would send content to the MCU that is outside the advertised capabilities of the MCU and therefore the MCU was unable to correctly decode it. Support for these content capabilities has been added in this release.
CSCtr80218	In previous releases, an MCU with gatekeeper setting as required, did not send an ARQ to its H.323 gatekeeper for an incoming call from a Microsoft Netmeeting client. This has been resolved in this release.
CSCtr80312	In previous releases, the active speaker indication was not shown in certain layouts. This has been resolved in this release.
CSCtr85035	In previous releases, under rare circumstances, the MCU configured with an old version of TMS could experience a restart if it ran out of web sessions. This has been resolved in this release.
CSCtr93658	In previous releases, uploading an invalid SSL certificate could result in a restart of the MCU. This has been resolved in this release.
CSCtu01703	In previous releases, when using a three blade MCU MSE 8510 cluster, under very rare circumstances some participants on a slave blade would receive black panes in their video output.

Identifier	Description
	This has been resolved in this release.
CSCtu04630	In Version 4.2, the MCU was using an ephemeral port range for both TCP and UDP of 10000 to 65535 instead of the documented range of 49152 to 65535. This has been resolved in this release.
CSCtu19596	When a conference created via an API call (for example, by Cisco TelePresence Management Suite (TMS)) uses a duplicate numeric ID to that of an existing ad-hoc conference on the MCU, the MCU correctly stops the conference from being created and generates the following error : "Failed to create conference" - duplicate numeric id". However, in previous releases, this error state continued even after the ad-hoc conference was deleted from the MCU. This has been resolved in this release.
CSCtw49855	In previous releases, when downloading a configuration file from the master MCU in a cluster which is heavily loaded with participants, in rare circumstances the slave MCUs could restart because of loss of contact with the master MCU. This has been resolved in this release.
CSCtw49892	In previous releases, when attempting to join a conference using a ConferenceMe invitation link, the request would fail with the message: “Error: conference no longer exists” if the conference name included some special characters. This has been resolved in this release.
CSCtw52422	In previous releases, under certain conditions, the Polycom Viewstation endpoint was not able to register to the MCU’s built-in gatekeeper, and a warning message would appear in the event log. This has been resolved in this release.
CSCtw61034	In previous releases, when resuming a call to the MCU that was placed on hold by any C-series endpoint, other participants did not hear any audio from that endpoint. This occurred in some versions of the MCU Version 4.2 software release and when the RTP sequence numbers increased by more than 32000 on resume. This has been resolved in this release.
CSCtw72308	In previous releases, the participant join notification text was sometimes not seen by video participants when an audio-only participant joined the conference. This has been resolved in this release.
CSCtw95448	In previous releases, the MCU could reboot when a participant set as the focused participant for active streaming viewers disconnected. This has been resolved in this release.
CSCtx00682	In previous releases, when using QuickTime player to stream the content window, QuickTime would fail over HTTP if "redirect http to https" was enabled. This was because the MCU would incorrectly redirect the streaming request from HTTP to HTTPS and QuickTime player does not support this. This has been resolved in this release.
CSCtx29749	In previous releases of the MCU, when sending G.728 to an MXP based endpoint, a high-pitched noise was heard after approximately 30 minutes. This has been resolved in this release.
CSCtx34673	In previous releases, under rare circumstances, the MCU 4500 could fail due to a memory address being read incorrectly. This issue has been resolved in this release.

Open issues

The following issues apply to this version of the Cisco TelePresence MCU software:

Identifier	Description
CSCty77949	When an attempt has been made to overwrite a valid auto attendant banner image with an invalid image, the MCU may not subsequently be able to delete the valid banner image when a user deletes the associated auto attendant. This can lead to a situation where all the auto attendant banner space is used, but the images can not be deleted – preventing further banner image uploads.

Identifier	Description
	To avoid this issue, do not attempt to upload invalid images to the auto attendant banner. Banner images must be of JPG, GIF or BMP format. Progressive JPG images are not supported. The maximum file size and dimensions of the auto attendant vary for the different hardware platforms; consult the online help for more information.
CSCua09541	On occasion, the MCU can unexpectedly restart while trying to decode a large number of corrupted bit-streams.
CSCty91437	In some cases, the username instead of the display name of a SIP participant will be shown on the MCU web interface. This is because when a SIP UAC presents multiple names in the SIP header field, the MCU will prioritize the PAI field over the Contact or From header field and often the PAI field will only have username present but not a display name.
CSCtr53874	Slot 10 of the Cisco TelePresence MSE 8000 chassis does not support clustering in this MCU software release. However, slot 10 in the same chassis as a cluster can be used for a standalone blade of any type.
CSCts46406	If the MCU Ethernet interfaces are configured to have the same IP address and then you attempt to disable a service on one of the interfaces the service is still allowed, even though the web interface shows it set to disabled.

Limitations

Issues when removing the CompactFlash™ during operation

Removing the CompactFlash card while the MCU is in operation has been known to cause a restart.

Windows Media Player

Streaming a conference with Windows Media Player in multiple windows or tabs on the same browser will crash the browser. This is a known issue with Windows Media Player. If you need to stream more than one conference simultaneously, use a different player such as QuickTime or Real Player.

In addition, Windows Media Player 11 (WMP11) can display streams incorrectly when used as an embedded player with browsers other than Internet Explorer. This is a known incompatibility. In some cases, setting the video size of the main streaming video window (the Video size field in the Streaming page) to Large will correct the problem. To work around this issue, you can use QuickTime or RealPlayer instead of WMP, or use Internet Explorer instead of your normal browser.

The MCU does not support 64-bit versions of Windows Media Player. To work around this limitation, use a 32-bit version of Windows Media Player.

Streaming to QuickTime 7 causes problems with some browsers

Streaming to an embedded QuickTime player using the QuickTime 7.0 plus later option for the Player format on the MCU can cause certain browsers to crash or remain in the 'negotiating' state indefinitely. Affected browsers include: IE6; Firefox 1.5 (Mac and PC); Safari 2.0.3 and earlier, and Camino. IE7 and Safari 2.0.4 do not appear to be affected by this. Using the QuickTime 6.5 plus later option for the Player format on the MCU will allow streaming to QuickTime using any browser that supports a QuickTime plug-in.

Clustering limitations

Cisco TelePresence MCU Conference Director will only work with the master blade in a cluster.

If you are using Cisco Telepresence Management Server Version 12.6 or earlier to schedule conferences on clustered blades, only add the master blade to TMS. Do not add slave blades to TMS and remove from TMS any blade that you subsequently configure as a slave blade: you will need to reconfigure any scheduled conferences that were previously configured on slave blades as new conferences running on the master blade.

Uploading and downloading large files while heavily loaded

We recommend that you do not upload or download large files from the MCU while it is hosting active calls. Files such as CDRs, audit logs and code images should be transferred when there are few or no calls on the MCU.

Binary Floor Control Protocol on encrypted calls

The transmission of SIP content from the MCU using Binary Floor Control Protocol (BFCP) is not supported on encrypted calls. To allow content to be transmitted over SIP calls in a separate channel from main video, you should disable encryption on the MCU or on the target endpoint.

Raw IPv6 addresses in Firefox 4.0

It is not possible to access an MCU HTTPS web interface in Mozilla Firefox Version 4.0 using a raw IPv6 address. It is possible with IPv4 addresses and in earlier versions of Firefox, or if a hostname is used instead of the raw IPv6 address. This is being tracked by Mozilla as bug 633001.

Interoperability

We endeavor to make the MCU interoperable with all relevant standards-based equipment. While it is not possible to test all scenarios, the testing that the data below is based on covers all the most common functions of the listed endpoints and infrastructure.

Version 4.3(1.68) of the MCU software was used for this interoperability testing.

About the interoperability section

The interoperability section describes the equipment and software revisions that were tested for interoperability with this release. The absence of a device or revision from this section does not imply a lack of interoperability.

Interoperability testing often requires interworking from one signaling/call control protocol to another. The following table lists phrases that are used to briefly describe the call paths that were tested for each interoperability scenario. The explicit call paths in the table place the endpoint first and the MCU last as a general convention.

Call path phrase	Explicit call path description
SIP	Endpoint <--SIP--> MCU. A registrar is used but not shown here.
H.323	Endpoint <--H.323--> MCU. A gatekeeper is used but not shown here.
H.323 to SIP interworking	Endpoint <--H.323--> VCS <--SIP--> MCU.
SIP to H.323 interworking	Endpoint <--SIP--> VCS <--H.323--> MCU.
CUCM to VCS H.323	Endpoint <--SIP--> CUCM <--SIP--> VCS <--H.323--> MCU.
CUCM to VCS SIP	Endpoint <--SIP--> CUCM <--SIP--> VCS <--SIP--> MCU.

Note: Unless otherwise stated, CUCM version 8.6(1a) and VCS version X7.0 were used in the interoperability tests.

Endpoints

This section lists interoperability issues with endpoints, by manufacturer. Where an endpoint has limitations, such as a lack of support for encryption or content, the interoperability tests omitted the limitations and they are not listed here.

An infrastructure issue may manifest itself as an issue with a particular endpoint or series of endpoints; issues of this nature are listed separately under 'Infrastructure'.

Cisco endpoints

Equipment	Software revision	Comments
Cisco Cius	sipcius.9-2-1SEC	Tested SIP interoperability via CUCM-VCS trunk. No issues found.
Cisco E20	TE4.0.0	Tested SIP, SIP-H.323 interworking via VCS, and SIP via CUCM-VCS trunk. No issues found.
Cisco Jabber Video for TelePresence (Movi)	4.2.0	Tested SIP and SIP-H.323 interworking via VCS. ■ Jabber Video will display the video from the MCU in the wrong aspect ratio when using the H.263 codec. Under normal circumstances H.264 or H.263+ is used in preference to H.263. (CSCtx91864)
Cisco TelePresence System MXP 1700	F9.1	Tested H.323 and SIP interoperability. ■ This version of the MXP takes several seconds for FECC commands to become active when calling using SIP. (CSCty04059)
Cisco CTS 3000	1.8.0(34)	Tested SIP interoperability via CUCM-VCS trunk. ■ In rare circumstances, video shown on CTS can become corrupted. (CSCtx91858)
Cisco CTS 500	1.8.0(34)	Tested SIP interoperability via CUCM-VCS trunk. ■ In rare circumstances, video shown on CTS can become corrupted. (CSCtx91858)
Cisco C60, Cisco EX90	TC4.2.1	Tested H.323 and SIP interoperability. No issues found.
Cisco Unified IP Phone 9971	9.1(2)	Tested SIP interoperability via CUCM-VCS trunk. No issues found.
Cisco Unified Video Advantage	2.2(2.0)	Tested SIP interoperability via CUCM-VCS trunk. No issues found.

Polycom endpoints

Equipment	Software revision	Comments
Polycom HDX 8000	3.0.2.1-17007	Tested H.323 and SIP interoperability. ■ In a conference which is sending a content stream and the content stream changes to a different content provider, endpoints will receive data in a different codec. In the case of the Polycom HDX, the endpoint ignores all incoming packets. This also occurs if the content provider itself changes codecs, for example, if the computer providing the content changes resolution. (CSCtw49873 / Polycom: VIDEO-93014)
Polycom ViewStation SP	7.5.4	Tested H.323 interoperability. No issues found.

Equipment	Software revision	Comments
Polycom QDX 6000	3.0.2181	Tested H.323 interoperability. No issues found.
Polycom VSX 7000e	9.0.6.1	Tested H.323 interoperability. No issues found.
Polycom VVX 1500	3.2.2.0481	Tested H.323 and SIP interoperability. ■ Due to inaccurate timestamps sent by this endpoint, lip synchronisation cannot be guaranteed. ■ In some circumstances this endpoint can fail to display video during SIP calls. ■ On low bandwidth H.323 calls, the endpoint may not be able to decode audio.

Sony endpoints

Equipment	Software revision	Comments
Sony PCS-G50	2.64	Tested H.323 and H.323-SIP interworking via VCS. ■ Content is not supported when H.323-SIP interworking is via the VCS.
Sony PCS-1	3.42	Tested H.323 and SIP interworking. ■ Audio between the MCU and this endpoint is not supported on interworked calls if “Audio Mode:” setting on the endpoint is set to either “MPEG4 Audio” or “Auto”.
Sony PCS-HG90	2.20	Tested H.323 and H.323-SIP interworking via VCS. ■ Does not support two-way video at less than 410 kbps. ■ The Sony HG90 only supports video in 1280x720 resolution. If the HG90 is dialled in to a conference on the MCU, it will become an audio only call if the MCU is set to transmit video in 4:3 ratio only.
Sony PCS-XG80	2.31.00	Tested H.323 and SIP. ■ H.323 call to an encryption-required conference results in an audio only call. ■ The MCU does not support FECC with this endpoint when calling using SIP.

TANDBERG legacy endpoints

Equipment	Software revision	Comments
Tandberg Classic 6000	E5.3 PAL	Tested H.323 and H.323-SIP interworking via VCS. ■ Due to inaccurate timestamps sent by this endpoint, lip synchronization cannot be guaranteed. ■ Bandwidth must be set to 768k or lower in order for encryption to work.
Tandberg 150 MXP	L6.1.0	Tested H.323 and SIP interoperability. ■ The MCU does not support FECC with this endpoint when calling using SIP.

Other endpoints

Equipment	Software revision	Comments
Aethra X3	11.2.2	Tested H.323 interoperability. ■ Due to inaccurate timestamps sent by this endpoint, lip synchronisation cannot be guaranteed. ■ The MCU does not support SIP with this endpoint.
LifeSize Room	4.7.13(22)	Tested H.323 and SIP interoperability. ■ Encrypted SIP calls are not supported between the MCU and this endpoint (CSCtx91859). ■ SIP content is not supported between the MCU and this endpoint. ■ G.722.1 Annex C is not supported between the MCU and this endpoint.
Radvision Scopia XT1000	02.05.0031	Tested H.323 and SIP interoperability. ■ Encrypted SIP calls are not supported between the MCU and this endpoint.

Infrastructure

This section lists known interoperability issues with infrastructure components. These may manifest themselves as issues with a particular endpoint or series of endpoints.

Equipment	Software revision	Comments
Cisco TelePresence Video Communication Server (VCS)	X7.0	■ If a call is made between an endpoint and an MCU, with the endpoint using SIP and the MCU using H.323, and a second endpoint joins the conference and sends a content stream (any protocol) to the MCU, the first endpoint display will freeze or go black when the second endpoint stops streaming content. This is because the first endpoint is not aware that streaming has ended and is expecting to receive further content. (CSCtx71406) ■ An endpoint, for example CTS, may end up in a half encrypted call where the call leg from CTS > CUCM > VCS is unencrypted and the call leg from VCS > MCU is encrypted.
Cisco Unified Communications Manager	8.6(1a)	■ After using hold and resume, CTS endpoints connected via CUCM do not receive audio from the MCU (CSCtr60976). ■ In networks in which not all call legs are encrypted, calls may drop after using hold and resume. When using encryption it is recommended that all call legs are encrypted (CSCtr52491).
Cisco TelePresence Content Server	S5.0	Tested H.323 and SIP interoperability. ■ Audio may be distorted if G722.1 codec is negotiated. (CSCty01044) ■ Audio may be distorted on low bandwidth calls. (CSCtx91864)
Polycom MGC	9.0.4.3	Test H.323. ■ H.264 video between the MGC and the MCU is not supported if the call bandwidth is 384 kbps or less. To avoid this, either use a higher bandwidth or disable H.264 when dialing the MGC using custom codec selection.(Reference CSCts46389)
Tandberg Gatekeeper	N5.2	No issues found.

Equipment	Software revision	Comments
Polycom PathNav	7.00.03	No issues found.
GNU Gatekeeper	2.3.1	No issues found.

Updating to 4.3

Prerequisites and software dependencies

CAUTION: You **must** back up your configuration **before** upgrading to Version 4.3.

You must also remember the administrator user name and password for the backup configuration. You will need these if you ever need to make use of this backup file.

Upgrading causes all CDRs to be deleted. If you are using Call Detail Records (CDR) for billing, auditing or any other purpose, before you upgrade to this release, you must download and save your current CDR data. Also, if you downgrade from this release to any older version, the MCU will delete **all** existing CDRs.

Upgrade instructions

Using a web browser

1. Unzip the image file.
2. Browse to the IP address of the MCU using a web browser.
3. Log in as an administrator.
4. Go to the **Settings > Upgrade** page.
5. In the Main software image section, type in, or browse to the location of the software image file.
6. Click **Upload software image**.

   A progress bar is displayed in a separate pop-up window while the web browser uploads the file to the MCU or MSE media blade. This takes some time – dependent on your network connection. Do not move your web browser away from the Upgrade software page or refresh this page during the upload process; otherwise, it will abort.
   After a number of minutes, the web browser refreshes automatically and displays “Main image upload completed successfully”.
7. Click **Close Status window**.
8. In the changed Upgrade page, click **Shut down MCU**.
9. Click **Confirm MCU shutdown**.
10. When shutdown has completed, click **Restart MCU and upgrade**.
11. When prompted, confirm the restart. The unit will restart and upgrade itself – this may take up to 25 minutes to complete.

Using FTP

1. Use an FTP client to connect to the MCU – e.g. `ftp <MCU IP Address>` from the command prompt.
2. Log in as an administrator.

3. Upload the upgrade file from the command prompt. For example:

```
put codian_mcu_4.3(2.30)
```

4. When the upload has completed, go to the Upgrade page within the web interface.
5. Click **Shut down MCU and upgrade**.
6. Click **Confirm MCU shutdown**.
7. When shutdown has completed, click **Restart MCU and upgrade**.
8. When prompted, confirm the restart. The unit will restart and upgrade itself – this may take up to 25 minutes.

Note: If you have been logged out due to inactivity, log in again as admin and click **Restart MCU and upgrade** on the Shutdown page.

Notes

- The progress of the upgrade can be monitored through the serial port
- Before upgrading, make sure that the MCU is not in use. Anyone using the MCU at the time of the upgrade may experience poor performance and loss of connectivity

Downgrade instructions

If you need to reverse your upgrade, you can re-install the former version of the software. The downgrade procedure is the same as for the upgrade except that it uses the earlier software image.

Note: We do not support downgrading to MCU versions earlier than 4.0. The compulsory password protection included from that version onwards makes it impossible to log in to the MCU after a downgrade to an earlier version. If you are experiencing these circumstances, visit the Cisco support website.

⚠ **CAUTION:** If you use CDR data for any purpose you must download and save the CDR data before you downgrade to an earlier version.

To downgrade from release 4.3:

1. Go to **Settings > Upgrade**.
2. In the **Restore configuration** area, locate a *configuration.xml* file that is compatible with the release to which you want to downgrade.
3. Check the *User settings* check box.
4. If required, check the *Network settings* check box.
5. Click **Restore backup file**.
6. When the configuration has been restored, follow the instructions as detailed in *Upgrade instructions* above.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a Cisco.com username and password.

3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

4. Type the product name in the **Search** field and click **Search**.
5. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology*.

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

Getting help

If you experience any problems when configuring or using the MCU, see the "Product documentation" section of these release notes. If you cannot find the answer you need in the documentation, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

Document revision history

Date	Revision	Description
2012-01-12	03	Release notes for Release Candidate.
2012-02-07	04	Release notes for full release.
2012-02-15	05	Interoperability data added.
2012-03-08	06	Addition of issues resolved since Version 4.3(1.68).
2012-04-04	07	Release notes for version 4.3(2.18) (Maintenance release 1).
2012-07-06	08	Release notes for version 4.3(2.30) (Maintenance release 2).