Cisco TelePresence MCU 5300 Series Version 4.3(2.30)

Software Maintenance Release Notes
July 2012

Contents

Product documentation

- D14876 Cisco TelePresence MCU 5300 Series Getting started guide
- D14956 Cisco TelePresence MCU 5300 Series Product administration guide
- D14523 Cisco TelePresence Accessing Conferences Getting Started guide MCU 4.3
- D14663 Cisco TelePresence Call Detail Records File Format Reference Guide

New features in Version 4.3(2.17)

This document describes the features introduced in the first release of the Cisco TelePresence MCU 5300 Series software (4.3(2.17)) and then goes on to list open issues and issues resolved in later maintenance releases.

The MCU 5300 Series is an entry level range of standards-based multipoint control units (MCUs) that is compatible with all major vendors' standard definition (SD) and high definition (HD) endpoints. The MCU 5300 can be clustered and has a flexible port capacity allowing scalability according to your organization's telepresence usage.

The main features of the MCU 5300 Series are summarized below.

Design features

- Standards-based and compatible with all major vendors' endpoints
- Software selectable between HD or SD video ports
- Upgradable unit capacity using software port licenses
- Ability to cluster two units together for increased capacity
- Easy-to-use, versatile management interface
- More than 50 custom layouts
- Comprehensive wideband audio support
- Support for both Session Initiation Protocol (SIP) and H.323 endpoints
- Cisco TelePresence PacketSafe technology, which minimizes effects of network packet loss
- Compact size: One rack unit (1RU) tall and 19-in. rack-mountable

Application features

- Provides upscale SD resolution using Cisco TelePresence ClearVision technology
- Integrated with Cisco TelePresence Management Suite
- Offers full interoperability with ISDN networks using standalone Cisco TelePresence ISDN gateways (sold separately)
- Compatible with Microsoft Office Communications Server via Cisco TelePresence VCS (sold separately)
- Supports Cisco Multiway technology

Performance features

- Continuous presence on every port
- Cisco TelePresence Universal Port technology, which helps ensure each participant receives the best possible experience
- Predictable port capacity
- Bandwidth per site up to 4 Mbps
- Video resolutions up to 1080p, 30 frames per second

Clustering the MCU 5300

Up to two MCU 5300s can be clustered to increase capacity. The resulting cluster will provide the sum of the capacities of the individual units, for example, if you connect two MCU 5320s that each support 10 x 1080p participants you will have a cluster that supports 20 x 1080p participants.

One of the MCUs acts as the master unit and the second as a slave. In order to cluster MCUs you will need a stacking cable which must be ordered separately. Please contact your reseller or go to www.cisco.com.

Features compared with Cisco TelePresence MCU 4500 Series

The following table compares the feature set of the MCU 5300 Series to that of the MCU 4500 Series.

Feature	MCU 4500 Series	MCU 5300 Series
nHD (w360p) mode	Not available	Included
SD mode	Limited (4501 only)	Included
Hardware stacking	Not available	Available
Capacity upgrades using SW license keys	Limited (4501 only)	Available
ConferenceMe	Included	Not available
Web Conferencing Option (streaming support)	Included	Not available
Additional content/streaming ports in HD mode	Included	Not available
Built in Gatekeeper	Included	Not available
VNC (Virtual Network Computing) support	Included	Not available
G.723.1	Included	Not available
MCU Conference Director Option	Available	Not available
Asymmetric 1080p and MHD upgrade	Available	Not available

Open issues

The following issues apply to this version of the MCU 5300 Series.

Identifier	Summary
CSCts46406	If the MCU 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.

Resolved issues

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

Resolved since 4.3(2.17)

Identifier	Description
CSCua84353	In the previous release, the MCU 5300 could experience an unexpected restart after a long idle time. 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 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.
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.
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

Identifier	Description
	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.

Limitations

Uploading and downloading large files while heavily loaded

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

Interoperability with CTS endpoints

Using CTS Series endpoints with the MCU 5300 Series is not currently recommended.

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(2.17) 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.

Call path phrase	Explicit call path description
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(2a) and VCS version X7.1 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	Version	Results
Cisco Cius	sipcius.9-2-2-49	Tested: CUCM to VCS H.323 and CUCM to VCS SIP. No issues found.
Cisco IP Video Phone E20	TE4.1.1.273710	Tested: CUCM to VCS H.323 and CUCM to VCS SIP. ▪ If a conference that is sending content is placed on hold and then resumed, the content is seen in the main video pane after resume.(CSCty98376)
Cisco TelePresence Jabber Video (Movi)	4.3	Tested: SIP and SIP to H.323 interworking. ▪ 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) ▪ Encrypted calls may fail after being put on hold for more than 15 minutes and then resumed.(CSCtz01282) ▪ In some circumstances an encrypted call may fail if the user returns from the conference to the auto attendant. (CSCtz01369)
Cisco TelePresence System 1700 MXP	F9.1.2	Tested: H.323 and SIP. ▪ FECC negotiation can take several seconds on SIP calls. (CSCty04059)
Cisco TelePresence System 3000	1.8.1	Using CTS Series endpoints (version 1.8.1) with the MCU 5300 Series is not currently recommended.
Cisco TelePresence System 500 Series	1.8.1	Using CTS Series endpoints (version 1.8.1) with the MCU 5300 Series is not currently recommended.
Cisco TelePresence System Codec C60	TC5.0.1	Tested H.323 and SIP. No issues found.
Cisco TelePresence System SX20	TC5.1	Tested H.323 and SIP. No issues found.
Cisco Unified IP Phone 7985G	4.1(7)	Tested SIP and CUCM to VCS H.323. ▪ The endpoint may not be able to decode video from the MCU when H.263+ is negotiated. Under normal

Equipment	Version	Results
		circumstances H.264 is used in preference to H.263+.
Cisco Unified IP Phone 9971	9-2-3-27	Tested CUCM to VCS H.323 and CUCM to VCS SIP . No issues found. The MCU 5300 Series only supports Cisco Unified IP Phone 9971 running version 9-2-3-27 or later.
Cisco Unified Personal Communicator	8.5.4.19609-6.2.83	Tested CUCM to VCS H.323 and CUCM to VCS SIP. No issues found.
Cisco Unified Video Advantage	2.2.2.0	Tested CUCM to VCS H.323 and CUCM to VCS SIP. No issues found.

Polycom endpoints

Equipment	Version	Results
Polycom HDX 4500	3.0.3.1-19040	Tested H.323 and SIP. ▪ The Polycom HDX 4500 is unable to decode video or content sent by the MCU in aspect ratios of 1600x1200 and 800x600. (CSCts46398 / Polycom reference: VIDEO-90136) ▪ Using *only* Siren 14 audio codec with this endpoint is not supported. However, if the MCU does not apply this restriction, the parties will successfully interoperate using a different audio codec. ▪ Using *only* H.263 with this endpoint is not supported. However, if the MCU does not apply this restriction, the parties will successfully negotiate H.263+ or H.264 instead. ▪ When a content stream's codec changes during a conference, for example, when the provider or resolution changes, the endpoint stops displaying the content stream. (CSCtw49873) ▪ The endpoint is not capable of simultaneously sending H.263+ main video and H.264 content. All other codec combinations work. ▪ Delay in opening audio channel to MCU can result in early part of voice prompt not being heard at the endpoint.(CSCtz01271) ▪ MCU does not support sending 60fps to this endpoint. (CSCtz12643)
Polycom ViewStation SP	7.5.4	Tested H.323 and H.323 to SIP interworking. No issues found.
Polycom QDX 6000	4.0.2	Tested H.323 and SIP. ▪ H.323 to SIP interworking is not supported. ▪ Video artifacts may be visible in calls using H.261 codec .
Polycom VVX 1500	3.2.2.0481	Tested H.323 and SIP. ▪ Due to inaccurate timestamps sent by this endpoint, lip synchronization 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	Version	Results
Sony PCS-G50	2.64	Tested H.323 and H.323 to SIP interworking. ▪ Encrypted interworked calls with this endpoint are not supported. (CSCtz12733)
Sony PCS-1	3.42	Tested H.323 and H.323 to 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	2.22	Tested H.323 and H.323 to SIP interworking. ▪ The MCU should be configured for HD calls only. ▪ MCU does not support sending 60fps to this endpoint.
Sony PCS-XG80	2.31	Tested H.323 and SIP: ▪ FECC is not supported over SIP. (CSCtz01910) ▪ H.323 call to an encryption-required conference results in an audio-only call. (CSCtz01360)

TANDBERG legacy endpoints

Equipment	Version	Results
TANDBERG Classic 6000	E5.3 PAL	Tested H.323 and H.323 to SIP interworking. ▪ Due to inaccurate timestamps sent by this endpoint, lip synchronization cannot be guaranteed. ▪ Encryption is not supported if the call bandwidth is greater than 768k. (CSCtz01365)
TANDBERG 150 MXP	L6.1	Tested H.323 and SIP. ▪ The MCU does not support FECC with this endpoint when calling using SIP.

Other endpoints

Equipment	Version	Results
Aethra Vega X3	11.2.2	Tested H.323 interoperability. ▪ Due to inaccurate timestamps sent by this endpoint, lip synchronization cannot be guaranteed. ▪ The MCU does not support SIP with this endpoint.
LifeSize Room 200	4.7.18	Tested: H.323, SIP, H.323 to SIP interworking, and SIP to H.323 interworking. ▪ Interworking is not recommended with this endpoint. It natively supports SIP and H.323. ▪ Encrypted SIP calls are not supported between the MCU and this endpoint (CSCtx91859).

Equipment	Version	Results
		▪ G.722.1 Annex C is not supported between the MCU and this endpoint. (CSCtz21139)
Panasonic KX-VC300	2.30	Tested SIP and SIP to H.323 interworking.. ▪ Encryption is not supported between this endpoint and non-Panasonic equipment. ▪ 1080p resolution is not supported between this endpoint and non-Panasonic equipment. ▪ Delay in opening audio channel to MCU can result in early part of voice prompt not being heard at the endpoint. (CSCtz02262) ▪ SIP call drops after the MCU sends an update message. (CSCtx29996)
Radvision SCOPIA XT1000	2.5.0208	Tested H.323 and SIP. ▪ Encrypted SIP calls are not supported. ▪ BFCP is only supported on inbound calls to the MCU. (CSCtz21165) ▪ The MCU does not support 60fps mode with this endpoint. (CSCtz21102)

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	Version	Results
Cisco TelePresence Video Communication Server (VCS)	X7.1	▪ When interworking between H.323 and SIP, the VCS does not perform offer/answer correctly for G.729 codecs. This can manifest itself as a lack of audio on interworked calls that use G.729 codecs. (CSCty97265) ▪ An endpoint may end up in a half encrypted call where the call leg from EP > CUCM > VCS is unencrypted and the call leg from VCS > MCU is encrypted.
Cisco Unified Communications Manager (CUCM)	8.6(2a)	▪ No video received from Cius when Cius dials in via CUCM and is interworked to H.323 by VCS. (CSCty51760) ▪ 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	S5.3	Tested H.323 and SIP. No issues found. The MCU 5300 Series only supports Cisco TelePresence Content Server running version S5.3 or later.
Cisco TelePresence MCU 4200 Series Cisco TelePresence MCU 4500 Series Cisco TelePresence MCU MSE Series	4.3(1.68)	Tested H.323 cascading. ▪ Cascading is not supported between MCU 5300 and other MCU platforms running 4.3(1.68) or earlier. Cascading is supported when those MCUs are running version 4.3(2.18) or later. (CSCtz03995)
Polycom MGC	9.0.4.3	Tested H.323. ▪ H.264 video between the MGC and the MCU is not supported if the call bandwidth is 384kbps or less. To avoid this, either use a higher bandwidth or disable H.264 when dialling the MGC using custom codec selection. (CSCts46389)
Tandberg Gatekeeper	N5.2	No issues found.
Polycom PathNav	7.00.03	No issues found.
GNU Gatekeeper	2.3.1	No issues found.

Updating to 4.3(2.30)

Prerequisites and software dependencies

CAUTION: You **must** back up your configuration **before** you upgrade.

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

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.

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.

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 5300 Series, 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	01	First draft of the software release notes for EFT.
2012-02-27	02	Second draft for EFT2.
2012-03-05	03	Draft for Release Candidate 1.
2012-03-27	04	Draft for Release.
2012-04-18	05	Release version. 4.3(2.17).
2012-07-06	06	Maintenance release, 4.3(2.30). Added issues resolved since 4.3(2.17).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.