



# **Cisco TelePresence System C/SX/EX/MX/Profile Series**

Software release notes TC7

---

D1507103

January 2014

# Contents

<b>Contents.....</b>	<b>2</b>
<b>Document revision history .....</b>	<b>4</b>
<b>Introduction software version TC7.....</b>	<b>5</b>
Important notes and warnings for this software version .....	5
Provisioning support.....	5
Extended BFCP port range and Active Control ports .....	5
Hardware compatibility .....	5
Camera firmware .....	6
Camera firmware TC7.0.2, TC7.0.1 & TC7.0.0.....	6
<b>New features and functionality in TC7.0.2 .....</b>	<b>7</b>
<b>New features and functionality in TC7.0.1 .....</b>	<b>8</b>
<b>New feature descriptions TC7.0.1 .....</b>	<b>9</b>
<b>New features and functionality in TC7.0.0 .....</b>	<b>10</b>
<b>New feature descriptions TC7.0.0 .....</b>	<b>11</b>
Support for MX300 G2 including Touch 10" .....	11
New GUI for MX300 G2 .....	11
Support TMS phone book when provisioned by CUCM .....	11
Serviceability: Ethernet statistics on Touch.....	11
IPv6 and dual stack support.....	11
New diagnostic checks.....	12
Changes to the syslog feature.....	12
Presentation will stop when presentation source is disconnected .....	12
Password protection of the Touch administrator menu.....	13
<b>Open and resolved caveats in TC7 .....</b>	<b>14</b>
Using the Bug Search Tool.....	14
Resolved caveats in TC7.0.2.....	14
Resolved caveats in TC7.0.1.....	15
Resolved caveats in TC7.0.0.....	16

---

Open caveats in TC7.0.2.....	18
Open caveats in TC7.0.1.....	19
Open caveats in TC7.0.0.....	20
<b>Known limitations .....</b>	<b>22</b>
Cisco.....	22
<b>Interoperability .....</b>	<b>27</b>
H.323 gatekeepers/traversal servers .....	27
SIP registrars/proxies .....	27
Gateway interoperability .....	28
MCU interoperability .....	28
Streaming servers .....	30
Endpoint Interoperability.....	31
<b>xAPI Changes .....</b>	<b>34</b>
<b>Cisco TelePresence systems hardware dependencies .....</b>	<b>35</b>
Introduction .....	35
NAND Flash.....	35
Integrated camera .....	35
Using the xAPI / tshell to identify software limitations .....	37
Using the TAN Number to identify software limitations .....	38
EX series and MX series .....	39
C series and Quickset Series.....	40
<b>Cisco TelePresence Touch 8 hardware dependencies.....</b>	<b>42</b>
New hardware revisions for Cisco TelePresence Touch 8 .....	42
<b>Cisco TelePresence Touch 10 hardware dependencies.....</b>	<b>44</b>
<b>References and related documents .....</b>	<b>45</b>
Software filenames .....	45

## Document revision history

Revision	Date	Description
03	January 24 <sup>th</sup> 2014	Release of TC7.0.2, minor release
02	December 17 <sup>h</sup> 2013	Release of TC7.0.1, release for all TC endpoints
01	November 25 <sup>th</sup> 2013	Release of TC7.0.0, MX300 G2 only release

# Introduction software version TC7

This release note describes the features and capabilities included in the Cisco TelePresence System C/MX/EX/SX/Profile series codec software version TC7.

TC7.0.0 is only released for MX300 G2 in production and will not be released on [www.cisco.com](http://www.cisco.com).

TC7.0.1 and later supports all TC endpoints.

## Important notes and warnings for this software version

### Provisioning support

When using CUCM provisioning, the endpoint cannot register to a VCS (SIP or H323) at the same time. This use-case is not supported by Cisco. When CUCM provisioning is active, H323 mode is disabled. Cisco recommends TelePresence customers to migrate from H323 to SIP.

### Extended BFCP port range and Active Control ports

From TC7.0, BFCP and Active Control port will dynamically use ports from the RTP port range instead of 5070-5077 and 5170-5177, which was previously used.

## Hardware compatibility

This section is only relevant when using older software. TC7 is not affected.

Due to replacement of hardware components, there are some constraints on running older software on newly manufactured endpoints and Touch 8 devices. This is due to end-of-life of some components and introduction of new components that require changes in the software. Executing the API command “xstatus SystemUnit Hardware Module CompatibilityLevel” will reveal if there are any constraints on the system. For a detailed list of compatibility levels and software constraints for the Cisco TelePresence systems, please see the appendices in this document:

[Cisco TelePresence Systems hardware dependencies](#)

[Cisco TelePresence Touch 8 hardware dependencies](#)

A lock on endpoints and Touch 8 devices prevents the system from downgrading to unsupported versions. If a downgrade attempt fails, it may be due to lack of endpoint support or lack of Touch 8 support in the old software.

## Camera firmware

PrecisionHD 1080p4x S2 and PrecisionHD 1080p2.5x cameras are only supported with the SX20.

With C series codecs, these cameras will work as third party cameras. The C series codec software is not able to upgrade the camera and it is therefore not supported for usage with C series codecs.

The use of Cisco PrecisionHD 1080p4x S2 and PrecisionHD 1080p2.5x cameras as USB cameras is currently not supported. This will be supported for SX20 in a future release (current target TC7.1).

### Camera firmware TC7.0.2, TC7.0.1 & TC7.0.0

Camera type	Hardware ID	Software	First released in
PrecisionHD 1080p4x	52000000	S01752-2.0 FINAL ID: 20012 Sangam.pkg	TC 5.1.5
PrecisionHD 1080p2.5x	54000000	S01777-2-1 RC 3 ID: 20022 A7camera.pkg	TC7.0.0
PrecisionHD 1080p4x S2	53000000	S01777-2-1 RC 3 ID: 20022 A7camera.pkg	TC7.0.0
PrecisionHD 1080p12x	50000001 50000002 50000003 50000004	S01718-4.0 FINAL ID: 40083 Rover.pkg	TC5.1.6

## New features and functionality in TC7.0.2

- ▶ No new features have been introduced in TC7.0.2

## New features and functionality in TC7.0.1

- ▶ Feature preview of Mobile and Remote Access. This feature requires CUCM 9.1.2 (or later), Cisco Expressway 8.1 or Cisco VCS 8.1 (or later) in addition to an endpoint running TC7.0.1.



# New feature descriptions TC7.0.1

## Feature preview of Mobile and Remote Access

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows Cisco TC endpoints to have their registration, call control and provisioning services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The Expressway or VCS Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The Mobile and Remote Access solution requires CUCM 9.1.2 (or later), Cisco Expressway X8.1 or Cisco VCS X8.1 (or later) in addition to an endpoint running TC7.0.1. Please refer to the Remote Access via Expressway Deployment guide or Mobile Remote Access via Expressway Deployment guide for configuration instructions.

For a list of limitations please refer to the Cisco Expressway X8.1 or Cisco VCS X8.1 release notes and the known limitations section in this release note. Please refer to the TC Software Administrator Guide for instructions on how to configure Mobile Remote Access on the endpoint.

## New features and functionality in TC7.0.0

- ▶ Support for MX300 G2 including Touch 10
- ▶ New GUI for MX300 G2
- ▶ Support TMS phone book when provisioned by CUCM
- ▶ Serviceability: Ethernet statistics available on Touch
- ▶ IPv6 and dual stack support
- ▶ New diagnostic checks
- ▶ Changes to the syslog feature
- ▶ Presentation will stop when the presentation source is disconnected
- ▶ Password protection of the Touch administrator menu

# New feature descriptions TC7.0.0

## Support for MX300 G2 including Touch 10”

Please refer to [www.cisco.com](http://www.cisco.com) for information about the new MX300 G2 TelePresence system.

## New GUI for MX300 G2

TC7.0 includes a new visual design for the Touch control panels. The Touch 8 will use the visual design as the new Touch 10 for MX300 G2.

The C series codecs will continue to have the traditional GUI when using the OSD interface and remote control.

## Support TMS phone book when provisioned by CUCM

TC software now supports using TMS phone book while provisioned by CUCM

Previously TMS refused to provide a phonebook to a CUCM provisioned endpoint. This behavior will be changed in TMS 14.4 release.

A device pack for CUCM will allow TC7 endpoints to specify TMS as the phone book source for CUCM registered endpoints. This device pack will be released time after TC7 is released.

## Serviceability: Ethernet statistics on Touch

When the Touch panel is not paired to a codec, it is now possible to see the Ethernet statistics. This can be used to verify that the Touch has an IP address and is receiving and sending packets to the network.

You can also detect if packets are not received, and if packets are lost due to dropping and errors. This can help discovering network problems that cause issues in calls and lead to fewer endpoints mistakenly being RMA'ed.

## IPv6 and dual stack support

IPv6 and Dual stack operation is now fully supported, also when using ActiveControl and ICE.

To enable Dual stack operation with IPv6 as preferred protocol:

- xConfiguration Network 1 IPStack: Dual – Enables IPv4 and IPv6 network address (default).
- xConfiguration Conference 1 CallProtocolIPStack: Dual – Enables dual stack operation for the call protocols

- xConfiguration SIP PreferredIPMedia: IPv6 – selects which IP version to prefer for media if both versions are supported on both ends
- xConfiguration SIP PreferredIPSignaling: IPv6 - selects which IP version to prefer for signaling if both versions are supported on both ends.

## New diagnostic checks

The following diagnostic checks have been added in TC7.0:

- CallProtocolDualStack – Issues a warning if xConfiguration Conference[1] CallProtocolIPStack is set to a Protocol on which it does not have an IP address, or is set to Dual and only has an IPv4 or an IPv6 address.
- UdpPortRangeViolation - If the range is set to less than 100 or the end port is a lower number than the start port, a diagnostic warning is given and the default ports will be used.
- CameraPairing – Gives a warning if the codec has lost the connection to a network-paired camera. (Applicable in TC7.1.0 and later)

## Changes to the syslog feature

Some changes have been made to the syslog configuration in TC6.3 and 7.0. The following API status and configuration have been added:

- xConfiguration Security Audit Server Port Assignment: <Auto/Manual>
- xStatus Security Audit Server Port – shows the destination port number to the server.

The default value for port assignment is now Auto, which will use UDP port 514 for external unsecure communication and Tls (TCP) port 6514 for external secure communication. This is according to RFC5425. Prior to TC6.3, external unsecure syslog used TCP port 514 as the default port. This means that when upgrading to TC6.3 or TC7.0, the syslog server needs to be configured to listen to UDP instead of TCP. If any port numbers other than the default port are configured, the port assignment xConfiguration must be set to from Auto to Manual after upgrading. This change has been made to be compliant with IANA. When using Manual assignment, the port is set by the Audit Server Port value. This will use UDP for unsecure and TCP for secure communication. A restart is no longer needed for changes made to the xConfiguration Security Audit settings.

## Presentation will stop when presentation source is disconnected

If a presentation source is disconnected or goes into standby (e.g. a PC), the presentation will automatically be ended after 10 seconds. If the source is connected or comes out of standby within 10 seconds, the presentation will automatically be resumed.

## **Password protection of the Touch administrator menu**

You must sign in with the video system's administrator password to get access to the Administrator menu on Touch 8 and 10.

# Open and resolved caveats in TC7

## Using the Bug Search Tool

You can use the Bug Search Tool to find information about caveats (bugs) for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats. Not all bugs that are fixed or open are shown in the release notes. Bugs that are not deemed relevant are left out, but can be found in the Bug Search Tool.

To use the Bug Search Tool, follow these steps:

**Step 1** Access the Bug Search Tool by navigating to <http://www.cisco.com/cisco/psn/bssprt/bss>

**Step 2** Log in with your Cisco.com user ID and password.

**Step 3** To look for information about a specific problem, enter the bug ID number in the 'Search for bug ID' field, then click 'Go'.

## Resolved caveats in TC7.0.2

[Link to TC7.0.2 open caveats](#)

Reference ID	Endpoint	Component	Summary
CSCum24631	All	API	On TC 7.0.1, if you enable HTTPS and disable HTTP and then restart the system, you will not be able to access the web interface.
CSCum41362	All	API	Replies from the codec do not match the API description documents for TC 7.0 once you run the command <code>xCommand Phonebook Search Phonebooktype:corporate Offset:0 Limit</code> . The word "PhonebookSearchResult" is added in every row of data.
CSCul79409	SX20 MX300G2	Application	Receiving 4:3 presentation on SX20 leads to empty layouts for overlay/Single families. After pressing the LAYOUT CONTROL > Overlay (or Single) button from remote, TV output goes away (empty) and both main and presentation video are not shown.
CSCum34718	C-series and SX20 when using remote control	Application	When upgrading an endpoint to TC7.0.1, the endpoint shows a persistent "connection to touch screen is lost" on-screen message, although the endpoint never used a touch screen. The message can be cleared, but reappears after the system is booted.
CSCum70952	MX Series	Camera	In some rare cases the zoom motor in MX200/MX300

Reference ID	Endpoint	Component	Summary
			cameras times out. This is observed shortly after a reboot, after a software upgrade. The user will see a blurry image.
CSCuj88498	All	Edge	In a Collaboration Edge network, an ad hoc conference through the CUCM fails to get established when the client external to the enterprise tried to initiate the conference.
CSCum04312	All	H323	TC System may not be able to receive H323 calls if network connectivity is lost and regained a few moments later.
CSCum46306	EX Series SX20	Platform	Factory reset not working as expected via the Power button. Endpoints with this functionality are: EX60, EX90 and SX20. The pinhole button is not affected. After two or three attempts the factory reset will occur, but it will have the side effect of deleting the options key file.
CSCum70892	All	Platform	A Cisco TelePresence TC system may not reboot after crash in TC7.0.1.
CSCul81053	All	Platform	Configuration profiles do not take change on the next reboot.
CSCul48235	SX20	Video	Video from SX20 on CTMS is poor when switching as the active speaker. This appears as multiple back-to-back refresh frames.
CSCum34767	All	Web Interface	Apostrophe in system name/h323 alias/SIP URI causes blank system information web page

## Resolved caveats in TC7.0.1

[Link to TC7.0.1 open caveats](#)

Reference ID	Endpoint	Component	Summary
CSCuj70294	C-series	Camera	If connecting a 1080p camera as camera 1 and a 720p camera as camera 2 and then disconnecting the cameras and reconnecting in opposite positions only camera 1 is detected.
CSCub20591	All	Platform	When placing H323 calls between Cisco TelePresence codecs, the call may drop if there is a firewall located between the codec and the device (VCS for example) that is handling the h225 signaling. Cisco TelePresence codecs use H245 round-trip request and response sent every 30 seconds as a keepalive. Not all firewalls will monitor the H245 session of a H323 and this can causes issues where

Reference ID	Endpoint	Component	Summary
			calls will drop after some amount of time; for example 30 minutes.
CSCul48235	SX20 MX300G2	Video	Video from SX20 on CTMS is poor when switching as the active speaker. This appears as multiple back to back refresh frames.
CSCuj20978	All	Platform	On rare occasions the C60 is unable to decode all of the packets from a CTS endpoint in a point-to-point call. The CTS endpoint is sending bursts exceeding the Denial Of Service trigger point of 28packets in 1 ms and is dropping packets for 100ms. The limit is in 7.0.1 set to 40 packets in 1 ms, which resolves this issue.
CSCuj93939	Endpoints paired with Touch 8/10	Touch 8 Touch 10	Support for entering Polish Special Characters from Touch.
CSCul19747	MX300G2	Touch 10 Performance Mic 20	Touch 10 and Performance Mic 20 are not lit and not active when not in call. Mute is only available when in call.
CSCul32675	All	Phonebook	xCommand Phonebook Search does not respect Offset/Limit parameters. This means that you will only display 50 entries in the phone book at a time. If you search you will only see the first 50 matches of the search, so the searches would need to be more specific if the contact does not appear.

## Resolved caveats in TC7.0.0

[Link to TC7.0.0 open caveats](#)

Reference ID	Endpoint	Component	Summary
CSCui33371	All	Application	Cisco Touch device used with Cisco TelePresence codecs does not have any notifications in the system logs when the Touch device loses pairing.
CSCuj33951	All	Application	xStatus SystemUnit Uptime does not match the system uptime.
CSCuj49485	Profile T1	Audio	The C90 in a T1 system is not activating its audio inputs with



Reference ID	Endpoint	Component	Summary
			TC6.2. Only first 2 microphones are working.
CSCUj16288	All	Protocol	Multiway fails when codec is registered to SIP proxy 2. SIP outbound is configured with VCS redundancy. When proxy 1 is available, multiway is ok, but when proxy 1 is down multiway does not work through proxy 2.
CSCUl15447 CSCUl12967	Touch 8	Touch UI	The layout stage on the Touch panel appears mirrored compared to what is seen on the screen when Arabic is chosen as language.
CSCue58498	Touch 8	Touch UI	Touch panel not displaying Polish special character correctly when English language is used.
CSCue05564	All	Video	TC endpoint sending black video to MCU conference when entering a PIN enabled conference when dialling over VPN.
CSCUl13056	Endpoints using EM	Application	If an extension mobility enabled endpoint is not SIP registered and you try to sign in, it will timeout and show error dialog.
CSCUj14268	All	SIP	Peer SSL certificates are not validated for incoming calls even if TLS verification is enabled. While the calls are encrypted, no authentication of the originating endpoint is performed.
CSCUl12893	All	Platform	TC codecs hang when xConfiguration Logging Mode is set to Off because the queue it is writing to is full. Eventually the codec will become unresponsive and it has to be manually rebooted to recover.
CSCuc83847	Touch 8	Platform	When a network-connected Endeavour connects to the TC software endpoint it has been paired with via SSH, it does not verify the SSH host public key of the endpoint.
CSCUl02181	Touch 8	Platform	Ntpd is sometimes losing the time sync causing the Touch time to drift. This may cause problems with e.g. OBTP meetings.
CSCUj39031	Touch 8	Touch UI	In TC5, you could search folder wise on the Touch. This is useful for large deployments when you want to restrict the search to a specific folder. In TC6 you will always search the whole directory. The folder specific search is still available on OSD, which is inconsistent.
CSCUl17511	All	Web Interface	The maintenance mode web interface is partly broken in TC6.3 if the codec is booting into maintenance mode. Reboot/shutdown commands do not work.

## Open caveats in TC7.0.2

[Link to TC7.0.2 resolved caveats](#)

For open caveats regarding other endpoints/vendors, see the [interoperability](#) section. Use the Bug Toolkit to see more details and possible workarounds.

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
CSCum73083	C series	7.0.x	7.1.0	Automatic presentation selection is choosing main video source as the presentation  Source in some situations: out of standby, after ending a call. To fix, toggle presentation off and on.
CSCum67376	EX90	7.0.x	7.1.0	If DVI is selected as the main source, PC input is not played out locally and not sent to the far end. If DVI is used as the presentation source (default) there is no problem.
CSCum17873	SX20	6.3.x 7.0.x	7.1.0	SX20 - Cannot create/save several configuration profiles.
CSCuj68248	EX90	6.x 7.x	7.1.0	SIP Registration may be lost when doing heavy file transfers to a PC connected to the network via the PC port of the EX90.
CSCul83650	Touch 8"	All	7.1.0	Intermittent freezes observed, typically when accessing the system after it has been cleaned with moisture.
CSCul50031	Touch 8"	6.3.0 7.0.1	7.1.0	Some custom layouts defined in TC console may cause Touch panel to end up in the spinning wheel connecting state.
CSCum67440	Touch 10"	7.0.1	7.1.0	An area may appear dead on the Touch 10" panel if this area of the touch has been touched during startup of the panel. In the startup phase, a touch calibration process takes place. If something is in contact with the touch at this time, this area may lose its function until the touch panel has been restarted.
CSCuj59881 / CSCui34799	MX200/MX300 EX60	5.x 6.x	7.1.0	An active call is established on MX200, MX300 or EX60 at 1080p30. When second audio call is added, maximum resolution supported is 720p.
CSCub01177	VCS registered TC endpoints	5.x 6.x	7.1.x	We should send the RPID header when registered to a VCS. Currently this is only done when SIP is set to CISCO (CUCM) mode.
CSCuc64777	All TC endpoints	5.1.x 6.x	7.1.x	Confusing call setup for point-to-point OBTP meetings. For the second participant joining, the

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
				answer button will change from Join Meeting to Incoming Call. When button is clicked a new message appear with two options; "join meeting and end current" or dismiss.
CSCug06492	All TC endpoints using 802.1x	All	7.1.x	A switch is configured with a default data VLAN on a switch port. It tags all packets, also EAP packets with the DATA VLAN. When xConfiguration Network 1 VLAN Voice Mode is set to Off we can read this packet even though it is tagged with VLAN. When we set VLAN mode to auto or manual we discard any packet that is not tagged with our VLAN.
CSCul71818	Touch 8 / 10	All	7.1.x	Touch freezes and reboots when audit logging is set to "external" to a non-working audit server. Only wallpaper is shown on touch LCD.
CSCug06474	All TC endpoints using 802.1x	All	7.1.x	When using 802.1x and VLAN at the same time, we tag the EAP packets with a VLAN tag. The switch does not accept packets tagged with VLAN, hence 802.1x authentication fails.

## Open caveats in TC7.0.1

[Link to TC7.0.1 resolved caveats](#)

For open caveats regarding other endpoints/vendors, see the [interoperability](#) section.

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
CSCuj59881 / CSCui34799	MX200/MX300 EX60	5.x 6.x	7.1.0	An active call is established on MX200, MX300 or EX60 at 1080p30. When second audio call is added, maximum resolution supported is 720p.
CSCub01177	VCS registered TC endpoints	5.x 6.x	7.1.x	We should send the RPID header when registered to a VCS. Currently this is only done when SIP is set to CISCO (CUCM) mode.
CSCuc64777	All TC endpoints	5.1.x 6.x	7.1.x	Confusing call setup for point-to-point OBTP meetings. For the second participant joining, the answer button will change from Join Meeting to Incoming Call. When button is clicked a new message appear with two options; "join meeting and end current" or dismiss.
CSCug06492	All TC endpoints using 802.1x	All	7.1.x	A switch is configured with a default data VLAN on a switch port. It tags all packets, also EAP packets with the DATA VLAN. When xConfiguration Network 1 VLAN Voice Mode is set to Off we can read this packet even though it is tagged with VLAN. When we set VLAN mode to auto or manual we discard any packet that is not tagged with our VLAN.
CSCul71818	Touch 8 / 10	All	7.1.x	Touch freezes and reboots when audit logging is set to "external" to a non-working audit server. Only wallpaper is shown on touch LCD.

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
CSCug06474	All TC endpoints using 802.1x	All	7.1.x	When using 802.1x and VLAN at the same time, we tag the EAP packets with a VLAN tag. The switch does not accept packets tagged with VLAN, hence 802.1x authentication fails.

## Open caveats in TC7.0.0

[Link to TC7.0.0 resolved caveats](#)

For open caveats regarding other endpoints/vendors, see the [interoperability](#) section.

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
CSCul19747	Touch 10 Performance Mic 20	7.0.0	7.0.1	Touch 10 and Performance Mic 20 are not lit and not active when not in call. Mute is only available when in call.
CSCul32675	Touch 8	6.3.0 7.0.0	7.0.1	xCommand Phonebook Search does not respect Offset/Limit parameters. This means that you will only display 50 entries in the phone book at a time. If you search you will only see the first 50 matches of the search, so the searches would need to be more specific if the contact does not appear.  Workaround: Use detailed searches.
CSCuj93939	Touch 8	All	7.x	Support for entering Polish Special Characters from Touch.  Workaround: None
CSCuj59881	MX200/MX300 EX60	5.x 6.x	7.1.0	An active call is established on MX200, MX300 or EX60 at 1080p30. When second audio call is added, maximum resolution supported is 720p.
CSCub01177	VCS registered TC endpoints	5.x 6.x	7.1.x	We should send the RPID header when registered to a VCS. Currently this is only done when SIP is set to CISCO (CUCM) mode.
CSCuc64777	All TC endpoints	5.1.x 6.x	7.1.x	Confusing call setup for point-to-point OBTP meetings. For the second participant joining, the answer button will change from Join Meeting to Incoming Call. When button is clicked a new message appear with two options; "join meeting and end current" or dismiss.
CSCug06492	All TC endpoints using 802.1x	All	7.1.x	A switch is configured with a default data VLAN on a switch port. It tags all packets, also EAP packets with the DATA VLAN. When xConfiguration Network

Reference ID	Endpoint / Device	Versions affected	Fix Target	Description
				1 VLAN Voice Mode is set to Off we can read this packet even though it is tagged with VLAN. When we set VLAN mode to auto or manual we discard any packet that is not tagged with our VLAN.
CSCug06474	All TC endpoints using 802.1x	All	7.1.x	When using 802.1x and VLAN at the same time, we tag the EAP packets with a VLAN tag. The switch does not accept packets tagged with VLAN, hence 802.1x authentication fails.

# Known limitations

## Cisco

Reference ID	Equipment / Version	Summary
	Collaboration Edge	<p>The following limitations apply:</p> <ol style="list-style-type: none"> <li>1. Provisioning credentials are stored unencrypted on the endpoint in TC7.0.0. It is therefore very important to have the Administrator password set in order to prevent unauthorised access to these credentials. The Administrator password cannot be provisioned, so this has to be manually set on the endpoint. <b>Encryption of provisioning credentials is supported in TC7.0.1 and later.</b></li> <li>2. Administrator password cannot be provisioned</li> <li>3. No more than two TFTP addresses are supported. This limits the number of CUCM clusters to two behind one VCS Edge.</li> <li>4. Failover of CUCM or VCS/Expressway is not supported. <b>This may result in loss of registrations.</b></li> <li>5. Ad hoc conferencing on CTMS is not supported.</li> <li>6. There is no Edge provisioning wizard available when using OSD and remote control.</li> <li>7. CTI is not supported for Edge registered endpoints.</li> <li>8. One Button To Push (OBTP) meetings are not supported.</li> <li>9. Only TLS is supported as SIP Transport type. Encryption must be set to BestEffort.</li> <li>10. <b>CTMS conferencing for Edge collaboration endpoints is not supported. Cisco recommends to replace CTMS with TelePresence Server.</b></li> </ol> <p>The following configurations are mandatory in Edge mode:</p> <ol style="list-style-type: none"> <li>1. xConfiguration NetworkServices HTTPS VerifyServerCertificate: Off</li> <li>2. xConfiguration SIP Profile 1 TlsVerify: Off</li> </ol> <p><b>CSCum12629:</b> Extension mobility does not work for endpoints provisioned over Edge because the HTTP request to activate it is never sent.</p> <p><b>CSCum12572:</b> TC software uses the TFTPServer values in the Edge config response to find out what CUCM cluster to connect to. This doesn't work when you have a single Edge installation in front of multiple CUCM clusters. We need to use the UDS mechanism used by Jabber to look up the correct CUCM cluster per user.</p> <p><b>CSCum00288:</b> In a collaboration edge setup, a user ID cannot contain @, thus using e-mail address as user ID for provisioning is not working.</p>

		<p><b>CSCui33679:</b> Active control does not appear in GUI on a remote/mobile endpoint, which is registered through collaboration edge.</p> <p><b>CSCui25299:</b> TC software endpoint does not attempt re-provision when clustered VCS-E goes down. SIP registration times out and the edge endpoint is never attempting to re-provision. It should lookup DNS again and try to provision with another VCS-E in the cluster.</p> <p><b>CSCui40682:</b> Registration is lost in a failover setup when CUCM or VCS fails.</p> <p>If the CUCM subscriber or any VCS goes down, the endpoint's REGISTER attempt will fail. However, the endpoint never tries to register with the other CUCM node or through the other VCS-C. It continues to try re-registering with the primary CUCM over the first VCS node.</p> <p><b>CSCum71163:</b> The provisioning wizard is not available when using remote control. This means that Collaboration Edge must be configured in the web interface or from the command line (tshell). To configure Collaboration Edge on an endpoint without Touch the following configurations must be set:</p> <p>xConfiguration Provisioning Mode: Edge</p> <p>xConfiguration Provisioning LoginName:</p> <p>xConfiguration Provisioning Password:</p>
CSCui06180	Touch 8	<p>When having one H323 call on hold and one active H323 call there is no button appearing on the touch panel to merge the call.</p> <p>Workaround: Do not press the Hold button before merging calls</p>
CSCui35568	Web interface TC6.3 and newer	<p>Due to lack of cipher suite support in IE8 running on Windows XP, HTTPS access is no longer possible due to Cisco security requirements. Chrome, Firefox and Opera browsers work fine. These browsers have the necessary cipher suite support. IE8 works fine with Windows Vista, Windows 7 and Windows 8.</p>
CSCuj09795	Any	<p>When the system is set to localOnly in Presentation Policy setting, it does not send support for content in either SIP or H323, and it is not possible to receive presentation in a separate video channel. This is by design and will not be changed.</p>
CSCtq44757	Any	<p>The TC software is configured with the default SNMP</p>

		community strings. This is needed for "plug and play" functionality, but SNMP community strings should be treated as "credentials" and therefore this must be changed after initial configuration.
CSCue74341	TC6.0 and newer	The on-screen display interface in TC6 no longer has the option for double screen self-view available. This prevents setting self-view to full screen on a secondary monitor and prevents double screen self-view in a dual setup. Workaround: set the following configurations: xConfiguration Video SelfviewDefault OnMonitorRole: Second xConfiguration Video SelfviewDefault FullscreenMode: On
CSCue62534	TC6.1 and newer	The behaviour of the OSD is unpredictable when users are logged into the OSD with non-admin privileges. Most importantly, the ability to show or hide self-view does not work. The solution to this will be simple mode coming in TC7.1.
CSCug06474 CSCug06492	Any	802.1x authentication and VLAN's used in combination will not work properly and authentication will fail because EAP packets are dropped at the endpoint or at the switch side. Workaround is to disable VLAN on the codec and manually assign it on the switch port.
CSCue21526	Any	An incoming SIP call which is initiated as calltype:audio will appear as calltype:video on the receiving side. This is by design in SIP and it will therefore block a video port on the receiving endpoint instead of an audio port. The endpoint will therefore not be able to make a video call at the same time.
CSCud87999	PrecisionHD 1080p 4xS2 and Precision HD 1080p 2.5x with C-series endpoints	Precision HD 1080p4x S2 and Precision HD 1080p 2.5x are not upgradable or fully supported for C series. The cameras will operate as third party cameras. Camera control will work, but software upgrade is not possible.
CSCuc03476	Any	When moving from CUCM provisioning to VCS provisioning the wizard will not change the TlsVerify configuration and will still be On. Most likely this will result in a failing SSL handshake and a failover to TCP if default transport is set to Auto by the CUCM. A TCP registered endpoint will not be able to make secure calls.  Also CUCM provisioning will turn DisableListening on: xConfiguration SIP DisableListening: On. This setting has



		to be set to off in order for the endpoint to register to VCS. Additionally, CUCM requires ANAT mode On when using Dual stack, but when using VCS ANAT must be turned off. There is a diagnostic check for this configuration. When moving an endpoint between CUCM and VCS registration a factory reset should always be performed.
CSCuc09385	Endpoints registered to CUCM	Since a CUCM will not issue an "Install/Update LSC (Locally Significant Certificate)" request to the endpoint unless explicitly configured to do so, a factory reset will effectively hinder the endpoint from re-registering to the (same) CUCM after the reboot. The only recourse is for the system administrator to tick "Install/Update LSC" for the device in question on the CUCM side.
CSCtu99526	Any	There is a hardware incompatibility between the C-Series systems and some NEC monitors. So far this is seen with: NEC LCD4020 and NEC P401. This incompatibility will cause the monitor to wake up from sleep mode even if the codec is still in sleep. This happens when the monitor is connected using HDMI to HDMI. A workaround is to use the monitors DVI input.
CSCtr32420	Any	The C series codecs and units with such a codec inside it do not meet the Cisco password policy. It is highly recommended to set a password on the unit during install using the API command: 'systemtools passwd'
N/A	TC4.x and later	If the 'admin' user is deleted, the TMS will not be able to manage the system. At the same time the 'admin' user with a blank password will be recreated during next reboot if no other user with admin access exists.
N/A	TC4.x and later	xFeedback register Event/KeyDown masks the keys pressed on the remote control with a '*'. This is a security measurement to prevent key logging from the remote control. The '*' can be used to detect that someone has pressed a button on the remote control.
N/A	Cisco TelePresence Touch	The Cisco TelePresence Touch 8 must be connected to the same subnet as the codec it is pairing to.
CSCtr32348	PrecisionHD 1080p Camera all SW versions.	720p50, 720p30 and 720p25 output has no CRC included for HD-SDI. Depending on the device you connect the camera to, you may not get video using this format. The Cisco C Series codecs will support these formats.
N/A	Any	Startup scripts will not work with Windows end of line. You must use Unix end of line to be able to run multiple

		commands. Most editors have the option to set which format to use. If you use Notepad ++, you can set Unix format in the Settings/Preferences menu.
N/A	Any	If you run cascaded cameras and the chained cameras are running an old camera code, we have seen that zoom only works when trying to control the chained camera. The solution is to connect the cascaded camera as the first camera in the chain so that the camera is detected and upgraded by the codec, or use the Ethernet upgrade method.
N/A	Any	HD-SDI may not work with cables shorter than 3 meters. This is due to a jitter issue.
N/A	Any	The Cisco TelePresence codec C40/C60 (rev. 1) will not provide proper analogue VGA output for any resolution of 1080 lines or more.
CSCuj42385	TC6.2 and later	TC6.2 and later does not accept H323 dialing on the format @IPADDRESS. Workaround is to remove the @.
CSCud43145	TC5.x.x and TC6.x.x	It is not possible to take a web snapshot of a presentation when OSD mode is disabled on C20.

# Interoperability

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

## H.323 gatekeepers/traversal servers

Equipment	Software version	Comments
TANDBERG Gatekeeper	N6.1	
TANDBERG Border Controller	Q6.1	Both Assent and H.460.18/.19 traversal technologies are supported
Cisco TelePresence System Video Communication Server (VCS)	X6.1, X7.0.1, X7.1, X7.2	Both Assent and H.460.18/.19 traversal technologies are supported

## SIP registrars/proxies

Equipment	Software version	Comments
CUCM	8.6, 9.0, 9.1	<ul style="list-style-type: none"> <li>▶ Native registration. Encrypted calls are not supported in 8.6.</li> <li>▶ DTMF: KPML is not supported. If you use an H.323 Gateway to access a public telephone line, DTMF will not work. To resolve this:               <ul style="list-style-type: none"> <li>• Convert IOS Gateway to SIP or MGCP.</li> <li>• Insert a Unified Border Element between the CUCM and the H.323 Gateway to do SIP to H.323 conversion (CUCM-SIP-CUBE-H.323-GW).</li> </ul> </li> <li>▶ If you experience random call drops make sure the default maximum size for SIP message in CUCM is set to 11000 bytes (default is 5000 bytes)</li> <li>▶ If dual stream (BFCP) does not work:               <ul style="list-style-type: none"> <li>• Enable BFCP on SIP profile for endpoints in CUCM.</li> <li>• Enable BFCP for SIP trunk profile if calling to/from a Cisco VCS.</li> </ul> </li> <li>▶ NTP: Configure Unicast NTP references for endpoints in CUCM.</li> </ul>

		<ul style="list-style-type: none"> <li>► Provisioning: Make sure the endpoint has a DNS server that can resolve the host name, or change CUCM &gt; System &gt; Server, to be IP address instead of hostname.</li> <li>► CSCug19308: CUCM 8.6.2 directory returns more than the corporate limit set by the endpoint in the search. Fixed in CUCM 9.0</li> <li>► To get the correct call back number in call history for trunk calls between VCS and CUCM, make sure Directory URI's are used on every endpoint and that a top level domain is specified in the Enterprise Parameters of the CUCM. Otherwise endpoints will show DN@CUCM_IP in history instead of URI@domain.</li> </ul>
Cisco TelePresence System Video Communication Server (VCS)	X6.1, X7.0.1, X7.1, X7.2, X8, X8.1	If you configure a trunk towards CUCM 8.6 or 9.0, you must create a custom SIP trunk that does not remove BFCP lines towards CUCM. If you choose CUCM as profile in the VCS, BFCP will be removed and dual stream (BFCP) will not be possible between CUCM and VCS.

## Gateway interoperability

Equipment	Software version	Comments
Cisco ISDN LINK	IL1.1.0	CSCUh75104: Placing or receiving calls via ISDN Link from a TC6.2 system registered to VCS with ICE enabled results in no media at the far end ISDN system. This has been fixed in TC6.3. Pairing TC codec with ISDN Link requires an IPv6 address (link local). If IPv6 is disabled, pairing will fail.
TANDBERG MPS Gateway	J4.6, J4.7	CSCuc81894: C series codec shows black screen momentarily in a MPS voice switch conference when switching between 4:3 image and 16:9 image
TANDBERG Gateway	G3.2	
Cisco ISDN GW 3241	2.1	
RadVision Gateway B40	5.6.0.0.4	

## MCU interoperability

Equipment	Software version	Comments
-----------	------------------	----------

Cisco TelePresence Server 7010	3.0, 3.1	<p>CSCud79767: Content from CUCM registered C series endpoints can take 10 seconds to arrive at TS. Fixed in TS 2.42</p> <p>CSCue88488: TC based endpoint running TC6.0 software or later where a low level of packet loss is present on the network may experience the video session call rate down speed in attempts to mitigate the effects of the packet loss. The amount of down speeding experienced may be significant compared the to relative packet loss being experienced. With Clearpath enabled on the endpoint this issue should not be a problem in TelePresence server 3.1. Workaround is to disable RTCP TMMBR by putting it in the capability set filter of the endpoint: xConfiguration Experimental CapsetFilter: RTCP-Feedback-TMMBR</p> <p>CSCud91075: Sometimes you get an Encoder/Decoder mismatch. TelePresence Server 2.2 is prone to this issue and upgrading the TelePresence Server to 3.x will in many cases resolve the problem.</p> <p>CSCuh38547: Clearpath not working correctly between TelePresence Server 3.1 and SX20 if SX20 is initiating the conference. Fixed in TC6.3.0</p>
Cisco TelePresence Server MSE 8710	3.0, 3.1	CSCud79767, CSCue88488, CSCud91075 and CSCuh38547: See description above
TANDBERG MPS	J4.5, J4.6	CSCuc81894: C series codec shows black screen momentarily in a MPS voice switch conference J4.6 when switching between 4:3 image and 16:9 image
TANDBERG MCU	D3.10	
Cisco MCU 53xx	4.4(3.42)	Tested with TC5.1.4
Cisco MCU 42xx	4.4 (3.42)	
Cisco MCU 45xx	4.4(3.42)	
Cisco CTMS  <b>Cisco recommends customers to move to the TelePresence</b>	1.9	<ul style="list-style-type: none"> <li>▶ CSCul48235: When an SX20 is in a call on CTMS and becomes the active speaker, the video is very poor for the first few seconds. This is not a problem on other endpoints as SX20 has a different decoder. This also applies to MX300G2.</li> <li>▶ When dialing to the CTMS, VCS cannot be interwork the call (H.323 to SIP conversion). This conversion will make the call drop.</li> <li>▶ 1.9: Using a call rate below 1152kbps will result in CIF video in a</li> </ul>

<b>Server platform due to the number of caveats between the TC endpoints and CTMS and the end of life of CTMS.</b>		<p>CTMS conference</p> <ul style="list-style-type: none"> <li>▶ Endpoints that require the HD option key (SX20 and C20) and do not have it installed will not be able to receive presentation from CTS devices in CTMS conferences.</li> <li>▶ CSCuj13986: TC endpoints (except EX60) without Premium Resolution option key do not display presentation sent from any CTS endpoint in a CTMS conference.</li> <li>▶ TC interoperability must be enabled on the CTMS.</li> <li>▶ Black Screen Codes are supported, but these will not work if the system is behind a firewall.</li> <li>▶ CSCud36845: CTMS cannot handle mid call re-invite. This causes problems in mixed 720p/1080p environments</li> <li>▶ CSCud45692: CTMS does not respect capability set from a 720p restricted C series endpoint. This may cause no video after the 15-minute session refresh because the 1080p30/720p60 capable endpoints will start transmitting this resolution, which the 720p endpoint cannot decode.</li> <li>▶ Multisite is not supported when doing CTMS conferences</li> </ul>
Polycom RMX	7.8.0.246	<p>Basic SIP/H323 call OK</p> <p>Encrypted calls: no audio on C/EX/MX/SX series (CSCuh50078), blocky video on SX20 (CSCuh32320) – both bugs are fixed in TC6.2.1</p> <p>BFCP OK</p>
RadVision Scopia Elite	7.5, 8.0	BFCP does not work

## Streaming servers

Equipment	Software revision	Comments
Cisco TelePresence System Content Server	S4.1, S5.1, S5.2, S5.3	

## Endpoint Interoperability

Equipment	Software version	Protocol	Comments
Cisco TelePresence System 500series 3x00series 1x00series TX9000 TX9200 TX1310	1.9.3 (Ten Bears)	SIP	<p>Encrypted calls supported with TC6</p> <p>CSCtz95144: TX9000 version earlier than 1.9.2 does not handle RTCP PLI on the BFCP channel, which results in no presentation.</p> <p>CSCue55134 (Fixed in TC6.3): Point-to-point call between MX200 and CTS EP. Video corruption can be observed after 1 or 2 minutes into the call. The artifacts can be zebra pattern, color off or blocky video does not smooth out. Corruption clears up with I-frame.</p> <p>This may also cause high jitter value reports on the CTS side.</p>
Cisco TelePresence System CTS500-32 TX1300 TX9000 TX9200	TX6.0.2 (Lago)	SIP	<p>1080p60 support on Lago 1G codecs</p> <p>Encrypted calls supported with TC6</p> <p>CSCue12132: In a point-to-point call between TX9000 running TX6.0 and TC6 the TC6 endpoint has decoding errors on 1080p if the TX6.0 endpoint has previously dialed a CTMS.</p> <p>Bug is identified in TX software.</p> <p>CSCue55134: Point-to-point call between MX200 and CTS EP. Video corruption can be observed after 1 or 2 minutes into the call. The artifacts can be zebra pattern, color off, blocky video does not smooth out. Corruption clears up with I-frame.</p> <p>This may also cause high jitter value reports on the CTS side.</p> <p>CSCue31615: During a H.323 call between a CTS 500-32 system and a C40 system, if the CTS shares a presentation and then changes the presentation resolution to 640x480, the local presentation disappears. The remote C40 system can still see the presentation.</p>
Cisco TelePresence System MXP	F9.3.1	H.323/SIP	CSCuh25060: TC6.1 endpoint calling via H.323 through VCS to an MXP fails to connect due to "master slave negotiation failure".
TANDBERG Personal Series	L6.1	H.323/SIP	CSCtr32423: If you dial a TANDBERG 150 with software version L5.1.1 or older that has encryption

			setting set to 'on', you may not get audio in any direction.
Cisco IP Video Phone E20	TE4.1	SIP/H.323	
LifeSize Team 200/220	4.11.13(1) , 4.7.17(1).	SIP/H323	<b>CSCuj57861</b> : Sx20/C-series is not able to show presentation from Lifesize Team when Lifesize sends high resolution PC content and TC endpoint does not have a Premium Resolution option key installed. Fixed for SX20 in TC7.0.2.
LifeSize Room 200	LS_RM2_4.7.18 (15)	H.323/SIP	When encryption is set to Best Effort the call will not be encrypted on SIP. Workaround is to set encryption to 'On'. SIP/H.323 transfer does not work. SIP BFCP (dual stream) does not work.
LifeSize Express	LS_EX1_4.7.18 (15)	H.323/SIP	SIP transfer/hold does not work. LifeSize is unable to start presentation (BFCP).
LifeSize Passport	LS_PP1_4.8.0 (59)	H.323/SIP	SIP/H.323 transfer does not work.
Sony PCS-1	03.41	H.323/SIP	Dual stream is limited to 1 FPS. The main video frame rate will never exceed 15 FPS.
Sony PCS-XG80	2.31.00	H.323/SIP	SIP Far End Camera Control does not work. SIP encrypted calls does not work. SIP/H.323 transfer does not work. Sony is unable to start presentation (BFCP).
Radvision XT5000	3.0	H323/SIP	1080p60 does work – Fixed in Radvision 3.1.1. SIP Hold causes XT5000 to hang up call after 30s. BFCP does not work FECC does not work.
Microsoft Lync	2013	SIP over VCS trunk from VCS x8	Requires VCS x8 released September 2013
Microsoft OCS 2007R2 clients	2007 R2	SIP over VCS trunk	Maximum resolution CIF unless used with Cisco TelePresence Advanced Media Gateway (720p 30fps Maximum)  CSCue00022: TC software not able to send Media toward OCS due to problem with xConfiguration



			<p>Video Layout RemoteLayoutFamily: PresentationSmallSpeaker. Fixed in TC6.1.0</p> <p>CSCud07398: Calls from an SX20 (5.1.x) to OCS (2007r1) in either direction provide poor video on the SX20 side, and no video on the OCS side. No issues found in OCS 2007R2. OCS 2007R1 is not supported.</p>
Polycom VSX 7000	9.0.6.1	H.323/SIP	<p>At a low video rate and with main video set to sharpness the VSX will not display any video.</p> <p>SIP/H.323 transfer does not work.</p> <p>H.264 is only used on lower bandwidths.</p> <p>CSCuh27649: EX60 running TC6.1.1 intermittently receives no audio from Polycom VSX 8000 when H323 calls are made.</p>
Polycom HDX 8000 HD	3.0.5	H.323/SIP	<p>SIP Transfer does not work (not supported by Polycom).</p> <p>H323 transfer reported as "cannot connect" even when successful.</p> <p>SIP BFCP/TCP has flaws. This is fixed in Polycom HDX 3.0.5 and later because BFCP/UDP will be preferred.</p>

## xAPI Changes

xAPI changes are no longer published in the release notes. Please refer to the Cisco API Reference Guide available at

[http://www.cisco.com/en/US/partner/products/ps11422/prod\\_command\\_reference\\_list.html](http://www.cisco.com/en/US/partner/products/ps11422/prod_command_reference_list.html)

# Cisco TelePresence systems hardware dependencies

## Introduction

Due to replacement of hardware components there are some constraints running older software on newly manufactured endpoints. This is due to end-of-life of some components and introduction of new components that require support in the software. There are two ways to identify the minimum software version of a system, using the xAPI/tshell or by looking at the TAN number. These methods are presented in the following. Downgrading to an unsupported software version will fail. **The latest software releases are always backward compatible with all hardware versions.**

## NAND Flash

The Cisco TelePresence endpoints except SX20 and MX300G2 are using a NAND flash memory for general storage and transfer of data. Several versions of this NAND flash have been used in production. For simplicity in this document we will call the first flash version 0, the second flash version 1 and the third flash (expected Summer 2014) version 2. Endpoints that have version 1 of the flash memory must run software TC3.1.5 and later, 4.2.0 and later or 5.0.0 and later. Endpoints that have version 2 of the flash memory must run software TC5.1.9 and later, TC6.1.2 and later or TC7 and later.

If your endpoint does not have the CompatibilityLevel command or it returns compatibility level 0 it has the flash version 0 installed. This means that any software version can be installed on the system. When the compatibility level is higher than 0, a newer software release is needed. Version 2 of the flash memory will be identified by software compatibility level 4. **Please refer to the compatibility level table for further details.**

## Integrated camera

For units with an integrated camera (EX60/EX90 and MX200/MX300) the camera software is embedded into the application software. Units shipped with the E4 sensor cannot be downgraded or upgraded to any software version lower than TC4.2.4 or TC5.1.1 unless support is specifically documented in the release notes for the software you are downgrading to. Although 5.1.1 can be installed, Cisco recommends TC5.1.6 due to major color calibration improvements for MX series with the E4 sensor. CSCud31649.

To check which camera sensor the EX series or MX series product has, execute the API command "xStatus camera HardwareID".

**Example:***xStatus camera HardwareID**\*s Camera 1 HardwareID: "e3:0xd30a"**\*\* end*

If a system shipped with the E4 sensor is attempted to downgrade to an unsupported software version, the software downgrade will fail and the unit will reboot, keeping its existing software version. This example showed an EX60 with the E3 sensor, which means it can be downgraded to versions prior to TC 5.1.1.

## Using the xAPI / tshell to identify software limitations

Executing the API command **xStatus SystemUnit Hardware Module CompatibilityLevel** will reveal if there are any software constraints for the system.

The result returned when running the command will be 0, 1, 2, 3, 4, v, 1v, 2v or 4v:

Compatibility level	Applicable systems	Description	Minimum software version			
			TC4 <sup>1)</sup>	TC5 <sup>3)</sup>	TC6	TC7
0	All except MX200 G2	No restrictions	All	All	All	All
0	MX300 G2	Product was introduced with TC7.0.0	None	None	None	7.0.0
1	All	The system has the new flash memory installed	4.2.0	All	All	All
2	EX/MX	The system has the new flash memory and the new E4 sensor	4.2.4	5.1.6 <sup>2)</sup>	All	All
2	SX20	Product was introduced with TC5.1.0	None	5.1.0	All	All
2	C20	A new hardware revision, minor change	4.2.3	5.1.1	All	All
3	SX20	A new hardware revision, minor change	None	5.1.6	All	All
3	C40	A new hardware revision, minor change	4.2.4	5.1.5	All	All
V	MX300	Product was introduced with TC5.0.1	None	5.0.1	All	All
1V	MX300	NAND flash version 1.	None	5.1.0	All	All

		Minimum software version TC5.1.0.				
2V	MX300	NAND flash version 1 and E4 sensor.	None	5.1.6 <sup>2)</sup>	All	All
4	All TC EPs except SX20/MX300G2	NAND flash version 2	None	5.1.9	6.2.2 / 6.3.0	All

<sup>1)</sup> Although listed in this table **TC4 is no longer supported** and should not be used by any customer.

<sup>2)</sup> Although TC5.1.1 can be installed, Cisco recommends TC5.1.6 due to major color calibration improvements for MX series with the E4 sensor. CSCud31649.

<sup>3)</sup> TC5 will shortly be end of support; customers should migrate to TC6 or TC7.

#### Examples of executing the API command:

xStatus SystemUnit Hardware Module CompatibilityLevel

System	Output	Minimum version
MX300	*s SystemUnit Hardware Module CompatibilityLevel: "v"	5.0.1
SX20	*s SystemUnit Hardware Module CompatibilityLevel: "2"	5.1.0
C40	*s SystemUnit Hardware Module CompatibilityLevel: "0"	No restrictions (Cisco recommends no lower than 4.2.4)

## Using the TAN Number to identify software limitations

By finding the TAN number of the system, it is possible to determine the software restrictions without executing the API command. Find the compatibility level from the TAN number in the tables below and look up the software constraints in the above table.

**EX series and MX series**

<b>System</b>	<b>TAN number</b>	<b>Camera Sensor</b>	<b>NAND version</b>	<b>Compatibility level</b>
EX60				
	800-35326-05	E3	0	0
	800-35326-06	E3	1	1
	800-35326-07	E3	1	1
	800-35326-08	E4	1	2
(new LCD)	800-35326-09	E4	1	2
(new LCD)	800-35326-10	E4	2	4
Non-crypto	800-36052-05	E3	0	0
Non-crypto	800-36052-06	E3	1	1
Non-crypto	800-36052-07	E3	1	1
Non-crypto	800-36052-08	E4	1	2
Non-crypto (new LCD)	800-36052-09	E4	1	2
Non-crypto (new LCD)	800-36052-10	E4	2	4
EX90				
	800-35448-05	E3	0	0
	800-35448-06	E3	1	1
	800-35448-(07-10)	E4	1	2
	800-35448-11	E4	2	4
(New LCD)	800-35448-12	E4	2	4
Non-crypto	800-36051-05	E3	0	0
Non-crypto	800-36051-06	E3	1	1
Non-crypto	800-36051-(07-10)	E4	1	2
Non-crypto	800-35448-11	E4	2	2
Non-crypto (New LCD)	800-35448-12	E4	2	4
MX200				
	800-36834-02	E3	0	0
	800-36834-03	E3	1	1
	800-36834-05	E4	1	2
	800-36834-06	E4	2	4
Non-crypto	800-37182-02	E3	0	0
Non-crypto	800-37182-03	E3	1	1

Non-crypto	800-37182-05	E4	1	2
Non-crypto	800-37182-06	E4	2	4
MX300				
	800-36919-03	E3	1	V
	800-36919-04	E4	1	2V
	800-36919-05	E4	2	4V
Non-crypto	800-37822-03	E3	1	V
Non-crypto	800-37822-04	E4	1	2V
Non-crypto	800-37822-05	E4	2	4V

### C series and Quickset Series

System	TAN number	NAND version	Compatibility level
C20			
	800-35408-01	0	0
	800-35408-02	1	1
New USB chip	800-35408-02 D0	1	2
Non-crypto	800-36060-01	0	0
Non-crypto	800-36060-02	1	1
Non-crypto	800-36060-02		
New USB chip	D0	1	2
C40			
	800-34910-01	0	0
	800-34910-02	1	1
	800-34910-04	1	3
	800-34910-05	2	4
Non-crypto	800-36047-01	0	0
Non-crypto	800-36047-02	1	1
Non-crypto	800-36047-04	1	3
Non-crypto	800-36047-05	2	4
C60			
	800-35367-01	0	0
	800-35367-02	1	1
	800-35367-04	2	4
Non-crypto	800-36048-01	0	0
Non-crypto	800-36048-02	1	1
Non-crypto	800-36048-04	2	4



C90			
	800-35342-02	0	0
	800-35342-03	1	1
	800-35342-04	2	4
Non-crypto	800-36049-02	0	0
Non-crypto	800-36049-03	1	1
Non-crypto	800-36049-04	2	4
<b>SX20</b>	<b>TAN number</b>	<b>CPU revision</b>	<b>Compatibility level</b>
	800-36554-01	0	2
	800-36554-02	1	3
<b>MX300 G2</b>	<b>TAN number</b>	<b>CPU revision</b>	<b>Compatibility level</b>
	800-100474-01	0	0

# Cisco TelePresence Touch 8 hardware dependencies

## New hardware revisions for Cisco TelePresence Touch 8

There are as of TC7 four hardware levels of the Touch 8. The new hardware levels 1, 2 and 3 require newer software. From TC5.1.3 there is a lock preventing a downgrade of a system to a software version that is not supported by the connected touch panel.

The TAN number can be found on the back of the Cisco TelePresence Touch 8 panel on the sticker positioned in the upper right corner.



Identify the minimum software supported by using the TAN number with this table.

TAN number	Description	HW level	System type	Minimum release			
				TC4 <sup>1)</sup>	TC5 <sup>2)</sup>	TC6	TC7
800-35447-04	Touch sensor rev 1	0	EX	All	All	All	All
800-35343-05	Touch sensor rev 1	0	SX/C/Profile	All	All	All	All
74-9543-02	Touch sensor rev 1	0	MX	All	All	All	All
800-35447-06	OMAP rev 2	1	EX	4.2.4	5.1.4	All	All
800-35343-07	OMAP rev 2	1	SX/C/Profile	4.2.4	5.1.4	All	All
74-9543-04	OMAP rev 2	1	MX	4.2.4	5.1.4	All	All
800-38887-01	Touch sensor rev 2	2	EX	4.2.4	5.1.4	All	All
800-38886-01	Touch sensor rev 2	2	MX	4.2.4	5.1.4	All	All
800-38885-01	Touch sensor rev 2	2	SX/C/Profile	4.2.4	5.1.4	All	All
800-38887-02	OMAP rev 2 and Touch sensor rev 2	3	EX	4.2.4	5.1.4	All	All
800-38886-02	OMAP rev 2 and Touch sensor rev 2	3	MX	4.2.4	5.1.4	All	All

---

800-38885-02	OMAP rev 2 and Touch sensor rev 2	3	SX/C/Profile	4.2.4	5.1.4	All	All
--------------	--------------------------------------	---	--------------	-------	-------	-----	-----

<sup>1)</sup> Although listed in this table **TC4 is no longer supported** and should not be used by any customer.

<sup>2)</sup> TC5 will shortly be end of support; customers should migrate to TC6 or TC7.

# Cisco TelePresence Touch 10 hardware dependencies

The Touch 10 touch panel has currently no restrictions. It is introduced with MX300 G2 in TC7.0.0, so that is the minimum version. The Touch 10 is currently not supported with any other products than MX300 G2.

TAN number	Description	HW level	System type	Minimum release		
				TC7		
		0	MX300 G2	All		

## References and related documents

The following table lists documents and web sites referenced in this document. All product documentation can be found on our [web site](#)

Name	Document reference
Cisco website	<a href="http://www.cisco.com">http://www.cisco.com</a>
Cisco Software Download	<a href="http://www.cisco.com/cisco/software/navigator.html?i=1ch">http://www.cisco.com/cisco/software/navigator.html?i=1ch</a>
Cisco TelePresence User Documentation	<a href="http://www.cisco.com/go/TelePresence/docs">http://www.cisco.com/go/TelePresence/docs</a>

## Software filenames

The correct software filenames are listed in the following table.

TANDBERG TC system	Software for EX-series C-series MX200(G1) MX300 (G1)	Software for SX20 MX300G2	Serial number range
AES Encryption	s52000tc7_0_2.pkg	s52010tc7_0_2.pkg	All
No Encryption	s52001tcnc7_0_2.pkg	s52011tcnc7_0_2.pkg	All
AES Encryption (for CUCM)	cmterm-s52000tc7_0_2.cop.sgn	cmterm-s52010tc7_0_2.cop.sgn	All
No Encryption (for CUCM)	cmterm-s52001tcnc7_0_2.cop.sgn	cmterm-s52011tcnc7_0_2.cop.sgn	All

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](http://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.