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

Software release notes TC7

D1507126

May 2016

Contents

Document revision history

Revision	Date	Description
26	May 4th 2016	Added info about security vulnerability, and deferral notice
25	April 29th 2016	Release of TC7.3.6, minor release
24	January 20th 2016	Release of TC7.3.5, minor release with fix for bug CSCux85199
23	January 11th 2016	Minor corrections regarding the remote monitoring option key
22	October 23rd 2015	Minor release note updates regarding fix for bug CSCuu77466
21	October 19th 2015	Release of TC7.3.4, minor release
20	June 24th 2015	Minor corrections
19	June 24th 2015	Minor corrections
18	June 22th 2015	Release of TC7.3.3, minor release
17	May 13th 2015	Minor corrections regarding new naming for cop files
16	May 11th 2015	Minor corrections
15	March 18th 2015	Release of TC7.3.2, minor release
14	February 3rd 2015	Release of TC7.3.1, minor release
13	January 6th 2015	Minor corrections
12	December 19th 2014	Release of TC7.3.0
11	October 8th 2014	Release of TC7.2.1, fix for "Shellshock", general bug fixes
10	August 28th 2014	Release of TC7.2.0, FIPS certified
09	June 19th 2014	Release of TC7.1.4, fix for OpenSSL security issues
08	May 27th 2014	Release of TC7.1.3, fixes some FIPS related issues
07	May 13th 2014	Release of TC7.1.2
06	April 15th 2014	Release of TC7.1.1, fix for OpenSSL “Heartbleed” security issue
05	April 7th 2014	Release of TC7.1.0
04	January 27th 2014	Minor corrections in the section about alternate phonebooks, page 11
03	January 24th 2014	Release of TC7.0.2, minor release
02	December 17h 2013	Release of TC7.0.1, release for all TC endpoints
01	November 25th 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.

Important notes and warnings for this software version

TC7.3.6 - Discontinued support for TLS 1.0

Cisco TelePresence Endpoints running TC7.3.6 only support TLS version 1.1 and 1.2 due to security concerns with TLS version 1.0. Please note that this may affect communication with servers that only support TLS version 1.0. If TMS is running on a Windows server that only has TLS version 1.0 enabled by default (i.e. Windows Server 2008 R2) it may cause connection problems when the endpoints upgraded to TC7.3.6. Make sure TLS 1.2 or 1.1 is enabled on the server before upgrading to TC7.3.6. Older browsers may not be able to reach the endpoints web interface on HTTPS if the browser only supports TLS 1.0.

Upgrading to TC7.3.4 may break existing SSH connections requiring 3des-cbc algorithms

This specifically affects AMX integrations over SSH where the connection requires use of 3des-cbc. This algorithm has been removed from TC7.3.4 to address the security vulnerability CVE-2008-5161 - SSH Server CBC mode Ciphers Enabled (bug reference: CSCuu77466). Customers can use RS232 connection as an alternative to SSH to restore operation on TC7.3.4. Please contact AMX support for further inquiries.

From TC7.3.3 - Updated CA certificates for Collaboration Edge

The list of CA certificates recognized by the endpoint when connecting to the CUCM via Expressway (Collaboration Edge) infrastructure has been updated.

CAUTION: Please verify that the server certificates used by your CUCM via Expressway infrastructure are still recognized as valid before pushing this firmware to end user endpoints.

If the certificates are not valid, the MRA endpoint will not be able to provision and physical access to the endpoint might be needed to resolve the issue.

From TC7.3.2 – COP-files for CUCM are signed with RSA3

To improve software integrity protection, new public keys are used to sign cop-files for Cisco Unified Communications Manager Release 10.0.1 and later. To install a TC7.3.2 and later cop-file on a pre-10.0.1 Cisco Unified Communications Manager, consult the README for the ciscocm.version3-keys.cop.sgn to determine if this additional cop-file must first be installed on your specific Cisco Unified Communications Manager version. If these keys are not present and are required, you will see the error “The selected file is not valid” when you try to install the software package. A k3 extension has been added to the filename: cmterm-s52000tc7_3_2.**k3**.cop.sgn

ciscocm.version3-keys.cop.sgn can be found at the following location:

https://software.cisco.com/download/release.html?mdfid=283782839&reltype=all&relind=AVAILABLE&release=COP-Files&softwareid=282204704&sortparam=2

TC7.2.0 is the minimum software requirement for SX10

SX10 systems that are already on TC7.1.x should upgrade to TC7.2.0. After the upgrade has been completed the system can no longer be downgraded to TC7.1.x. There is a mechanism that prevents the system from downgrading to TC7.1.x once on TC7.2.x.

Provisioning support

When using CUCM provisioning, the endpoint cannot register to a VCS (SIP or H.323) at the same time. This use-case is not supported by Cisco. When CUCM provisioning is active, H.323 mode is disabled. Cisco recommends TelePresence customers to migrate from H.323 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.

Camera firmware

In the table below you can find an overview of the camera software included in the TC 7 software releases. If new camera software is included in a software release, it will be listed in the table below. If not listed, the camera software is the same as the previous release.

Release	Hardware name/ID	Software name/ID	Notes
TC7.3.6	Precision 60	HC7.3.6.ea51021	
TC7.3.5	N/A	N/A	
TC7.3.4	PrecisionHD 1080p 2.5x	S01777-2.2 RC12 [ID:20035]	
	PrecisionHD 1080p 4x S2	S01777-2.2 RC12 [ID:20035]	
	Precision 60	HC7.3.4.e4daf54	
TC7.3.3	Precision 60 55000000	HC7.3.3.c84180a	
TC7.3.2	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC7 ID:20030	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC7 ID:20030	
	Precision 60 55000000	HC7.3.2.14ad7cc	
TC7.3.1	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC6 ID:20029	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC6 ID:20029	

	Precision 60 55000000	HC7.3.1.e4d9a5c	
TC7.3.0	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC5 ID:20028	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC5 ID:20028	
	PrecisionHD 1080p 12x 5000000(1-4)	S01718-4.0 FINAL ID:40084	
	Precision 60 55000000	HC7.3.0.8cb420c	
TC7.2.1	Precision 60 55000000	HC7.2.1.9ddaa3b	
TC7.2.0	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC3 ID:20027	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC3 ID:20027	
	Precision 60 55000000	HC7.2.0.36dac2c4	
TC7.1.4	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC1 ID:20025	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC1 ID:20025	
	Precision 60 55000000	HC7.1.4.908e4a9a	
TC7.1.3	Precision 60 55000000	HC7.1.3.db40e557	
TC7.1.1 TC7.1.2	Precision 60 55000000	HC7.1.1.48db3d2	
TC7.1.0	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 Alpha1 ID:20023	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 Alpha1 ID:20023	
	Precision 60 55000000	HC7.1.0.48db3d2	
TC7.0.1 TC7.0.2	PrecisionHD 1080p 4x 52000000	S01752-2.0 FINAL ID:20011	
	PrecisionHD 1080p 2.5x	S01777-2-1 RC 3	

	54000000	ID:20022	
	PrecisionHD 1080p 4x S2 53000000	S01777-2-1 RC 3 ID:20022	
	PrecisionHD 1080p 12x 5000000(1-4)	S01718-4.0 FINAL ID:40083	

SX20 Quick Set and SX80 camera support

Codec	Camera	Support comments
SX20	PrecisionHD 1080p 2.5x	Full support
	PrecisionHD 1080p 4x S2	Full support
	PrecisionHD 1080p 12x	Full support
SX80	Precision 60	Full support
	SpeakerTrack 60	Full support
	PrecisionHD 1080p 4x S2	Full support
	PrecisionHD 1080p 12x	Basic usage with Pan Tilt and Zoom functionality is supported. * Software upgrade of this camera is not supported natively by this codec. * Daisy chaining cameras is not supported on SX80.

Note: An overview for other integrator systems will be available in a later document revision.

Deferred software versions

A software version is deferred when we find critical security issues within the software. This is to prevent users from downloading affected software versions. Replacement software will always be in place before a software version is deferred.

TC7.2.0, TC7.2.1, TC 7.3.2, TC7.3.3, TC 7.3.4 and TC7.3.5 deferral

Deferred 4th of May 2016.

Please read the deferral notice for more information.

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/cisco-tc720-tc721-tc732-tc733-tc734-tc735-deferral-notice.pdf

TC7.3.0 and TC7.3.1 deferral

Deferred 10th of April 2015.

Please read the deferral notice for more information.

https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/software-deferral-notice-tc730-tc731.pdf

TC7.0.0, TC7.0.2 and TC7.1.0 deferral

Deferred 3rd of June 2014.

Please read the deferral notice for more information.

http://software.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/software-deferral-notice-tc5-tc6-tc7.pdf

New features and functionality in TC7.3.6

- This is a minor release and contains bug fixes, including the critical security bug CSCuz26935 (CVE-2016-1387).

New feature and functionality descriptions TC7.3.6

TC7.3.6 fixes critical security bug CSCuz26935 (CVE-2016-1387)

Vulnerability in the XML Application Programming Interface (API) of the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) System Software could allow an unauthenticated, remote attacker to bypass authentication when accessing the XML API.

For more information, the Cisco Security team has published a security advisory regarding this bug: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-tpxml

The following vulnerable TC releases has been removed from Cisco.com:
TC7.2.0, TC7.2.1, TC7.3.2, TC7.3.3, TC7.3.4 and TC7.3.5

Cisco recommends all peers that are currently running one of the above software versions to upgrade to TC7.3.6 where this issue has been addressed.

New features and functionality in TC7.3.5

- This is a minor release and contains a bug fix for CSCux85199 only

New feature and functionality descriptions TC7.3.5

TC7.3.5 fixes a critical bug (CSCux85199) with SX20 Quick Set

On January 15th CE8.0.0 was deferred for Cisco TelePresence SX20 Quick Set due to an issue that broke the microphone mute button functionality after downgrading from CE8.0.0 to TC7.3.x. Note that some shipments of SX20 Quick Set may contain the same affected firmware even if the endpoint has TC7.3.x installed and have never been on CE8.0.0.

More details on the issue can be found in the software deferral notice:

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/ce8/release-notes/cisco_ce800_deferral_notice.pdf

If you are experiencing this issue and are running TC software you can upgrade to TC7.3.5 where this issue is resolved. Downgrading from CE8.0.1 to any TC7.3.x will not break the mute button functionality.

There are no other bug fixes in the TC7.3.5 release.

New features and functionality in TC7.3.4

- This is a minor release and contains bug fixes

New features and functionality in TC7.3.3

- This is a minor release and mainly contains bug fixes
- Remote Monitoring

New Feature Descriptions TC7.3.3

Remote Monitoring

This feature was previously known as Web Snapshots and can no longer be enabled from system settings in TC7.3.3.

A new option key that enables the Remote Monitoring feature has been introduced. This feature allows an administrator to monitor a room from the endpoint's web interface by getting snapshots from the camera sources connected to the endpoint.

The Remote Monitoring option key can only be added to systems that has upgraded to TC7.3.3 and above. Users attempting to add the option key to systems < TC7.3.3 will get an invalid option key message. Remote monitoring is enabled once the option key has been added and the system has been rebooted. Once this feature is enabled, the only way to disable it is to remove the option key.

This feature does not display warning messages or indicators on the local system that someone is monitoring the room, as it did in previous versions.

The option key comes at an additional cost and can be ordered with the following PID numbers:

PID*	Description
L-TP-RM	Remote Monitoring (Parent PID)
L-C-SERIES-RM	Remote Monitoring PID for C series
L-EX-SERIES-RM	Remote Monitoring PID for EX series
L-PROF-SERIES-RM	Remote Monitoring PID for Profile series
L-MX-SERIES-RM	Remote Monitoring PID for MX series
L-SX-SERIES-RM	Remote Monitoring PID for SX series

Note:

Example of a Remote Monitoring option key: 1S000-1-ABCD1234

New features and functionality in TC7.3.2

- This release includes a fix for the GHOST (CVE-2015-0235) and NTP.org (CVE-2014-9298) security vulnerabilities.
- This is a minor release and contains bug fixes only. Please see the open and resolved caveats sections for more details.
- Support for Cisco TelePresence MX800 Dual screen system.

New features and functionality in TC7.3.1

- This is a minor release and contains bug fixes only. Please see the open and resolved caveats sections.

New features and functionality in TC7.3.0

- Local preview of presentation in call
- SX80, MX700, MX800: Dual presentation outside call
- SX80, MX700, MX800 feature updates
- SX20: New passive mode OSD
- SX10 feature updates
- Web snapshots: Warn users when snapshots are being taken
- SpeakerTrack 60: Snap to Whiteboard
- Software upgrades via web will be faster
- Several other minor improvements

New Feature Descriptions TC7.3.0

Local preview of presentation in call

Allow the user to preview the presentation locally before sending to far end. This was available for EX systems previously, and is now possible across the portfolio.

SX80, MX700, MX800: Dual presentation outside call

When the system is not in a call, it can simultaneously display two different external sources on the connected screens (e.g. two laptops). This also includes the MX700 and MX800.

SX80, MX700 and MX800 feature updates

Several feature improvements to SX80, MX700 and MX800 to better align with C series functionality.

- H.323 / SIP dual registration is possible.
- Multiway is supported.
- Additional audio call is supported.

SX20: New passive mode OSD

Passive mode on SX20 (on-screen display when using a Touch control device) has an updated look and feel, to align with the rest of the portfolio.

SX10 feature updates

- Ad hoc conferencing support via Touch 10 or remote control.
- Extension mobility support on Touch 10.
- OBTP (One button to push) meetings now supported.

Web snapshots: Warn user when snapshots are being taken

On the web UI, there is a warning to the admin when using the camera snapshot feature that a notification will pop up on the screen of the endpoint when a snapshot is taken.

The system will also log when snapshots are taken, and which IP address the request was initiated from.

It is possible to allow/disallow snapshots remotely, but not to observe the room without the users being aware.

SpeakerTrack 60: Snap to whiteboard

This is a configurable option for better whiteboard scenario support.

When the system detects a person speaking close to a whiteboard, the camera will go to a pre-defined preset covering the whiteboard area as defined by the admin/installer.

There’s a setup wizard in the admin settings on the Touch 10. Please make sure to accurately measure the distance between the cameras and the whiteboard, and leave some space around the whiteboard itself to keep the person presenting in view.

Software upgrade speed improvements

Software upgrading an endpoint running TC7.3.0 (or later) via the web interface is roughly 80% faster than in TC7.2.x (and earlier). The software will be uploaded and installed immediately, there is no option to upload and then accept the upgrade manually. This was an option in previous software versions.

General improvements

- CDP can now be completely disabled.
- Historical log bundles will include (anonymized) call history by default.
- “xConfiguration Video Input Connector <X> PresentationSelection: Manual” will no longer cause the system to wake from standby even if a signal is detected.
- The flip-image-when-tilted functionality on EX cameras can now be disabled.
- New Touch 8 network-pairing mechanism that improves pairing stability. To use the new pairing mechanism the Touch 8 has to be un-paired and re-paired to the codec.

New features and functionality in TC7.2.1

- TC7.2.1 is mainly a bug fix release; please see the resolved caveats section for more information.
- This release includes a fix for CSCur02591 - TelePresence endpoint evaluation for CVE-2014-6271 and CVE-2014-7169 also known as the "Shellshock" bug.
- CEC support for SX10.

New feature descriptions TC7.2.1

CEC support for SX10

CEC standby control support has been added to SX10.

New features and functionality in TC7.2.0

- Support for Touch 10 network pairing for all new endpoints
- Improved failover support for endpoints registered through Collaboration Edge
- Intelligent Proximity with slide change detection on MX200 G2, MX300 G2 and SX20
- Added new provisioning parameters that can be provisioned from CUCM (10.5)
- Briefing room mode for specific room setups
- Improved language support for SX10 in active mode
- Collaboration Edge provisioning option added to the setup assistant of SX10
- OSD and touch panel screenshots can be captured from the web interface
- xStatus Video Output will print EDID information about the display
- FIPS certified software version

New feature descriptions TC7.2.0

Support for Touch 10 network pairing for all new endpoints

Network pairing of the Touch 10 is supported for the following endpoint models: SX10, SX20, SX80, MX200 G2, MX300 G2, MX700 and MX800. The network pairing process is similar to the one used on the Touch 8.

1. In order to pair the Touch 10 to one of the above codecs, the Touch 10 must be connected to a Power over Ethernet (PoE) enabled switch, or a PoE injector and to a network where the codec is reachable.
2. Once the Touch 10 has booted you will be asked to select the preferred language.
3. After language has been selected you will be presented with a pairing assistant.
4. You can type in the codec's IP address manually, or you can select the codec from the list of auto-discovered codecs.

   Note that the Touch 10 will only discover the codec for 10 minutes after the codec has booted. If the codec is not discovered, try rebooting the codec.
5. If the codec and Touch 10 software versions do not match, the Touch 10 will immediately start downloading touch panel software to match the codec version. The upgrade is automatic and the Touch 10 will reboot when the upgrade is complete.
6. The Touch 10 will prompt for a username and password after the reboot. Admin credentials of the codec are required.

The Touch 10 can be unpaired from the codec by accessing the Administrator Settings on the touch panel, select "Pairing", click the "Unpair" button and confirm.

Improved failover support for endpoints registered through Collaboration Edge

CUCM

If the CUCM is down, the endpoint will automatically re-register to another CUCM if available.

VCS Control and VCS Expressway

If the VCS Control or VCS Expressway goes down, the endpoint will automatically re-register to another VCS Control / VCS Expressway if available. Call preservation is not yet supported.

Provisioning (HTTPS)

If the provisioning service goes down, the endpoint will receive provisioning data from another provisioning service.

Phonebook

If the phonebook service goes down, the endpoint will automatically use another phonebook service.

Intelligent Proximity with slide change detection on MX200 G2, MX300 G2 and SX20

To save up to 80% battery consumption on the BYOD device, slide change detection has been ported to the codec. Please note that Cisco Proximity is still experimental. For support please visit the proximity support forums: https://supportforums.cisco.com/community/12156681/cisco-proximity.

New provisioning parameters can be provisioned from CUCM

The following configuration parameters can now be provisioned from CUCM under vendor specific configuration.

xConfiguration SystemUnit Name: <String>

xConfiguration Video OSD TodaysBookings: <On/Off>

xConfiguration Standby StandbyAction: <None/PrivacyPosition>

xConfiguration Audio DefaultValue: <0-100>

xConfiguration Conference 1 MaxTotalReceiveCallRate: <64-10000>

xConfiguration Conference 1 MaxTotalTransmitCallRate: <64-10000>

Briefing Room mode for specific room setups

A room mode has been introduced to support the Briefing room solution. By enabling the "Briefing" mode, the codec will activate a set of custom layouts and automatic behavioral control to work seamlessly with this specific room solution.

Please visit http://www.cisco.com/web/telepresence/projectworkplace.html to take a look at the "Briefing, Tokyo" room setup.

Improved language support for SX10 in active mode

SX10 in active mode (using the remote control) supports the same languages as the other TC endpoints except for the mirrored languages, e.g. Arabic. When the SX10 is paired to the Touch 10 the mirrored languages is supported.

Collaboration Edge provisioning option added to the setup assistant on SX10

The SX10 can now be provisioned through Collaboration Edge by selecting the "CUCM via Expressway" provisioning option.

Touch panel and OSD screenshots can be captured from the web interface

A new web feature has been implemented to be able to capture screenshots of the OSD and the touch panel. These screenshots can be used for e.g. troubleshooting, creating instructions or when identifying defects.

The feature is found under *Diagnostics / User Interface Screenshots* in the codec web interface.

Screenshots of OSD will be available for new endpoints (SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)

xStatus Video Output will now print EDID information about the display

In order to identify the connected display model and its preferred resolution *xStatus Video Output* will now print these values based on the EDID information. Please see the example below.

```
xStatus Video Output
*s Video Output Connector 1 Connected: True
*s Video Output Connector 1 ConnectedDevice Name: "BenQ E2420HD"
*s Video Output Connector 1 ConnectedDevice PreferredFormat: "1920x1080@60Hz"
```

FIPS certified software version

The product has met the requirements for FIPS 140-2 approved cryptographic module: Cisco FIPS Object Module (FIPS 140-2 Cert. #2100).

Please visit the following website for more details.

http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_fips140.html

New features and functionality in TC7.1.4

- AMX/Crestron integrators can now remove the "Touch Panel required" warning on SX80
- This release includes a fix for CSCup25163 - Multiple Vulnerabilities in OpenSSL - June 2014

New feature descriptions TC7.1.4

AMX/Crestron integrators can now remove the "Touch Panel required" warning on SX80

When a Touch 10 is not connected to SX80, the following warning will be displayed as default: "Touch panel required".

Integrators using AMX/Crestron instead of Touch 10 can avoid this warning message by using the following new configuration command:

```
xConfiguration Peripherals Profile TouchPanels: 0
```

This configuration sets how many touch panels the codec should expect. Setting it to "0" will remove the "Touch panel required" warning message. Fixes bug number CSCup34325.

New features and functionality in TC7.1.3

- A behavioral change in TC7.1.3 allows for software upgrades while the system is in FIPS mode.

New feature descriptions TC7.1.3

Software upgrade allowed in FIPS mode

A behavioral change in TC7.1.3 allows for software upgrade while the system is in FIPS mode. Preventing upgrade in FIPS mode is no longer required with the current FIPS validation. Cisco has decided to allow system upgrade while FIPS mode is enabled.

New features and functionality in TC7.1.2

- Support for MX700
- Support for MX800
- BYOD mode reintroduced as experimental configuration on EX, MX G1 series and C series

New feature descriptions TC7.1.2

Support for MX700

TC7.1.2 introduces support for the MX700 product.

Support for MX800

TC7.1.2 introduces support for the MX800 product.

BYOD mode reintroduced as experimental on EX, MX G1 and C series

BYOD Mode as an experimental configuration for EX, MX G1 and C series was removed from the TC7.1 release. This was due to performance limitations on those platforms. As the removal raised concerns that this would limit our abilities to demonstrate the value of this feature, we have decided to reintroduce the experimental BYOD mode configuration for the above products in TC7.1.2.

NOTE: This is an unsupported feature that will not see further development and bug fixing on the EX, MX G1 and C series platforms. This means that there will not be any TAC support for the feature itself, and TAC will request customers to turn off BYOD mode for problem resolution on other issues.

New features and functionality in TC7.1.1

No new features were introduced. TC7.1.1 is released to fix the OpenSSL “Heartbleed” issue.

New features and functionality in TC7.1.0

- Improved support for Collaboration Edge (CUCM), which includes UCM failover, improved messaging, TLS certificate verification, UDS support.
- Root account is now disabled permanently.
- Added support for the following devices:
  - SX10
  - SX80
  - SpeakerTrack 60
  - Precision 60 Camera
- For SX80 encrypted software is no longer a separate software package but is configured by installing a crypto option key.
- Serviceability: Ethernet statistics for codec is now available via touch.
- Support for dual registration with SIP and H.323 is removed for SX80, MX700 and MX800.
- New zoom range for PrecisionHD 1080p4xS2 and PrecisionHD 1080p2.5x
- xConfiguration Network 1 VLAN Voice Mode is now default set to Auto.
- xConfiguration Conference 1 Presentation Policy has been removed.
- Feature preview of Cisco Proximity.

New feature descriptions TC7.1.0

Improved support for Collaboration Edge (CUCM)

Collaboration Edge now supports CUCM UDS. User Data Service (UDS) is a service that provide access to user information stored in the Cisco Unified CM back-end storage

Collaboration Edge now supports and **requires TLS verification** for increased security. This means that the VCS-Expressway or Expressway-E needs to have a certificate installed that is trusted by the client (endpoint), and the VCS-Expressway and Control or Expressway-C and Expressway-E needs to have a trusted TLS connection. If the client cannot validate the certificate of the VCS-E or Expressway E, the endpoint will not receive the provisioning and not be registered. For details regarding certificate creation and deployment, please refer to “Cisco VCS Certificate Creation and Use Deployment Guide”. For additional details around setting up Collaboration Edge/Mobile Remote Access, please see:

- Cisco TelePresence VCS 8.1.1 Release Notes
- Cisco TelePresence VCS Administrator Guide or Cisco TelePresence Expressway Administrator Guide
- Cisco Mobile and Remote Access via VCS Deployment Guide or Cisco Mobile and Remote Access via Expressway Deployment Guide

Root account is permanently disabled

Cisco has decided to disable the root account completely for security reasons. A new restricted user "remotesupport" can be created on the endpoint. This user has read access to the system and a limited set of commands that can aid troubleshooting. The user can be created from the System Recovery section -> Remote Support User in the web interface. Once the user is created a token will be presented. To decode the token and acquire the password a Technical Assistance Center (TAC) case must be opened. The remote support user should only be enabled for troubleshooting reasons when instructed by the Cisco TAC.

Added support for new TelePresence products

Please refer to www.cisco.com for information about the following new devices:

- Cisco TelePresence SX10 Codec
- Cisco TelePresence SX80 Codec
- Cisco TelePresence SpeakerTrack 60
- Cisco TelePresence Precision 60 camera

Non-encrypted software is no longer a separate package

- For SX80 encrypted software is no longer a separate software package but is configured by installing a crypto option key.

Serviceability: Ethernet statistics for codec is now available via Touch

It is possible to get network statistics for the codec and touch panel from the administrator tab on the touch panel. This may improve troubleshooting touch pairing issues.

Dual registration SIP and H.323 is not possible on SX80, MX700, MX800

It is not possible to use SX80, MX700 and MX800 with both SIP and H.323 call protocols simultaneously. This is a feature limitation in this software version.

New zoom range for PrecisionHD 1080p4xS2 and PrecisionHD 1080p2.5x

- PrecisionHD4x S2 now has an increased zoom range to 8x by enabling 2x digital zoom. PrecisionHD2.5x now has increased zoom range to 5x by enabling 2x digital zoom.

xConfiguration Network 1 VLAN Voice Mode is now default set to Auto

An upgraded endpoint will get its VLAN Voice Mode value set to Off, if it was previously not configured. This will preserve the behavior for upgraded endpoints. If doing a factory reset or purchasing a new endpoint with TC7.1 or newer software, the default setting will be Auto, instead of off as previously. This means that an endpoint that was in the Data VLAN now may join the Voice VLAN (if available).

xConfiguration Conference 1 Presentation Policy has been removed

The xConfiguration Conference 1 Presentation Policy: <LocalRemote/LocalOnly> has been removed. To achieve the equivalent effect after the configuration removal, please use the following command: xCommand Presentation Start SendingMode: <LocalRemote/LocalOnly>.

Feature preview of Cisco Proximity

TC7.1.0 includes a feature preview of Cisco Proximity. To learn about what Cisco Proximity is and how to enable it, please visit http://cisco.com/go/proximity.

For Q&A and support, please visit https://supportforums.cisco.com/community/12156681/cisco-proximity.

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 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 for alternative phone book provisioning by CUCM

TC software now supports provisioning of an alternate phone book by CUCM

Previously the phone book type and address was set by default when provisioned to CUCM, this setting can now be modified to use a different phone book server type and address (TMS or UDS). Previously TMS refused to provide a phone book 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 96 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. **A subset of open or resolved bugs will no longer be listed in the release notes**. A pre-defined link will provide the correct and up-to-date list of open or resolved bugs. Please note that the "Series/Model" listed in the pre-defined search is universal and will list all bugs relating to all products that runs TC software.

To use the Bug Search Tool, follow these steps:

Step 1 Access the Bug Search Tool by navigating to *https://tools.cisco.com/bugsearch/*

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'.

Use the below links to access the open and resolved caveats lists for a specific software release.

Software version	Resolved caveats	Open caveats
TC7.3.6	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.6&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7&sb=anfr&sts=open&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.3.5	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.5&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.5&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.3.4	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.4&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.4&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.3.3	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.3&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.3&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.3.2	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.2&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.2&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.3.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.1&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.1&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV

TC7.3.0	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.0&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.3.0&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.2.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.2.1&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.2.1&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
TC7.2.0	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.2.0&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.2.0&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.1.4	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.4&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.4&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.1.3	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.3&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.3&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.1.2	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.2&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.2&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.1.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.1&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.1&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.1.0	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.0&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.1.0&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.0.2	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.0.2&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.0.2&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV
7.0.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.0.1&sb=fr&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=7.0.1&sb=afr&svr=3nH&scs=hSc&srtBy=svr&bt=custV

Known limitations

Equipment / Feature	Summary
CUCM	**Provisioning of administrator password** Administrator password cannot be provisioned from CUCM. **BugID: CSCun94641** CAPF Authentication mode by authentication string is not supported, if a Touch controller is not used. As a workaround, authentication string can be set on the web interface when it has been requested by the CUCM. Resolved in TC7.3.0.
Collaboration Edge	**Provisioning credentials** 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. Encryption of provisioning credentials is supported in TC7.0.1 and later. **TFTP addresses** No more than two TFTP addresses are supported. This limits the number of CUCM clusters behind one VCS Edge to two. **Ad-hoc conferencing with CTMS** Ad hoc conferencing on CTMS is not supported. **CTI Support** CTI is not supported for Edge registered endpoints. **OBTP** One Button To Push (OBTP) meetings are not supported. **Encryption** Only TLS is supported as SIP Transport type. Encryption must be set to BestEffort. Collaboration Edge cannot be used with Non-cryptographic TC software (TCNC). **CTMS Conferencing** CTMS conferencing for Edge collaboration endpoints is not supported. We recommend replacing CTMS with TelePresence Server. **BugID: CSCum12629** Extension mobility does not work for endpoints provisioned over Edge because the HTTP request to activate it is never sent. Resolved in TC7.2.0. **BugID: CSCum12572** TC software uses the TFTPServer values in the Edge configuration response to find out what CUCM cluster to connect to. This does not work when you have a single Edge installation in front of multiple CUCM clusters. The UDS mechanism, used by Jabber, has to be used to look up the correct CUCM cluster per user. Resolved in TC7.1.0.

	BugID: CSCum00288 In a Collaboration Edge setup, a user ID cannot contain @, thus using an email address as user ID for provisioning does not work. Resolved in TC7.1.0. **BugID: CSCul33679** Active control does not appear in GUI on a remote/mobile endpoint, which is registered through Collaboration Edge. Resolved in TC7.1.0. **BugID: CSCui25299** TC software endpoint does not attempt to re-provision when clustered VCS-E goes down and the Collaboration Edge DNS SRV record resolves to more than one host and the host name resolves to several IP addresses. In this case the TC endpoint will not re-provision. Closed. This scenario is not supported by the Collaboration Edge solution. **BugID: CSCui40682** Registration is lost in a failover setup when CUCM or VCS fails. If the CUCM subscriber or any VCS goes down, the endpoint's REGISTER attempt fails. 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. Resolved in TC7.2.0. **BugID: CSCum71163** The provisioning wizard is not available when using a remote control. This means that Collaboration Edge must be configured on the web interface or from the command line (tshell). To configure Collaboration Edge on an endpoint without a Touch controller the following configurations must be set: xConfiguration Provisioning Mode: Edge xConfiguration Provisioning LoginName: xConfiguration Provisioning Password: Resolved in TC7.2.0 (SX10) TC7.3.0 (SX20) with new OSD interface. **BugID: CSCuo60302** Endpoint loses registration for 15 minutes when the user password is changed on CUCM. This is due to a 15 minutes cache in the VCS-E for SIP credentials, and the lack of sync between the SIP and HTTP password. The endpoint will be provisioned, but it will not be able to register until 15 minutes later since the VCS-E is expecting the old password. Resolved with the combination of VCS X8.5, CUCM 10.5.1, TC7.3.0 and above.
TRC5 and TRC6 remote controls	**Unsupported devices** Remote control is not a supported control device for SX80, MX700, MX800, MX800 Dual and MX G2 series. A Cisco Touch 10 panel should be used with the above systems.
ISDN Link	**BugID: CSCuq64530** SX80 (TC7.2.0) using H.323 cannot place calls using ISDN Link. Resolved in TC7.3.0.

H.265	**General information** H.265 will only work with SIP and is currently only supported by the SX80, MX700, MX800 and MX800 Dual. **Interoperability** Some calls involving third-party endpoints might experience video issues when H.265 is included in the SIP SDP. The workaround is to disable H.265 on the endpoint.
Intelligent Proximity	**SX10 Intelligent Proximity limitations** Cisco Proximity will not receive presentations when paired with SX10 endpoints in this version. Endpoint control functionality is available. **Experimental feature only** Intelligent Proximity is not supported with endpoints running TC software. Only a limited experimental version of the feature is available. Support will be introduced with Collaboration Endpoint Software version 8.0.0. Inquiries and support: http://www.cisco.com/web/go/proximity-support
SX20 Quick Set	**Bug ID: CSCux85199** Microphone LED behavior is incorrect if an SX20 within a certain serial number range is downgraded from CE8.0.0 to TC software. The symptom is that the microphone LED glows red constantly even if the system is un-muted. *Resolved in CE8.0.1/TC7.3.5*
MX200/MX300 EX60	**BugID: CSCui34799** An active call is established on MX200, MX300 or EX60 at 1080p30. When second audio call is added, the maximum resolution supported is 720p.
Touch 10	**BugID: CSCum67440** An area may appear dead on the Touch 10 controller if the screen has been touched during start-up of the controller. In the start-up phase, a touch calibration process takes place. If something is in contact with the Touch 10 screen at this time, this area may lose its function until the Touch controller has been restarted. Do not touch the Touch controller during a boot to avoid this.
Active Control	**BugID: CSCuo88201** Active Control is now set to "Auto" by default. It was set to "Off" in previous releases. When set to “Auto”, the endpoint negotiates it, and if passing over VCS Trunk to CUCM 8.6.2, calls fail with 503 Service Unavailable. Active Control is supported on CUCM 9.1.2. To work around this issue: Disable Active Control with xConfiguration Conference 1 ActiveControl Mode: Off. Alternatively you can filter this from VCS, running X8.1.X, by changing Zone Profile to Custom, and setting SIP UDP/IX filter mode to ON.
Touch 8	**BugID: CSCui06180** When having one H.323 call on hold and one active H.323 call there is no button appearing on the Touch 8 to merge the call. Workaround: Do not press the Hold button before merging calls **BugID: CSCuu46149 and CSCum87923** Touch 8 might become sluggish over time when paired to the codec over network.

	This issue may happen on TC7.3.0 through TC7.3.2, but also below if the system has been downgraded from TC7.3.x. The bug prevents the Touch to send logs to the codec causing a memory leak that may lead to Touch sluggishness within 2-8 weeks. A reboot temporary resolves the issue. Both bugs are resolved in TC7.3.4 **Network pairing** The Touch 8 must be connected to the same subnet as the codec it is pairing to.
Web interface	**BugID: CSCul35568** Due to lack of cipher suite support in IE8 running on Windows XP, HTTPS access is no longer possible due to Cisco security requirements. On Windows XP the web interface can be used with Chrome, Firefox and Opera browsers. These browsers have the necessary cipher suite support. IE8 works with Windows Vista, Windows 7 and Windows 8. **BugID: CSCuw70703** TC7.3.x: Uploading certain customer wallpapers to an endpoint running s52000 software may in some situations cause an out of memory issue and the endpoint will crash. The workaround is to try to upload a different image. A fix for this issue is targeted for TC7.3.5.
Presentation	**BugID: CSCuj09795** When the system is set to localOnly in Presentation Policy setting, it does not send support for content in either SIP or H.323, and it is not possible to receive presentation in a separate video channel. This is by design and will not be changed.
SNMP	**BugID: CSCtq44757** The TC software is configured with the default SNMP community strings. This is needed for "plug and play" functionality, but SNMP community strings should be treated as "credentials" and therefore must be changed after initial configuration.
Selfview	**BugID: CSCue74341** The on-screen display interface in TC6 and later 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
On-screen user interface (OSD)	**BugID: CSCue62534** The behavior of the on-screen display is unpredictable when users are logged into the on-screen display with non-admin privileges. Most importantly, the ability to show or hide self-view does not work. Solution for this issue was introduced in TC7.1 for the SX10 on-screen display for TRC6.
VLAN	**BugID: CSCug06474 & CSCug06492** 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. A workaround is to disable VLAN on the codec and manually assign it on the switch port. Resolved in TC7.2.0.

Cameras	**BugID: CSCud87999** PrecisionHD 1080p4x S2 and PrecisionHD 1080p 2.5x are not upgradable or fully supported for C series. The cameras operate as third party cameras. Camera control will work, but software upgrade is not possible. **BugID: CSCtr32348** Applies to PrecisionHD 1080p Cameras with all software 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 C Series codecs support these formats. **Daisy chained camera upgrades (does not apply to SX80)** 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. **HD-SDI cable length** HD-SDI may not work with cables shorter than 3 meters. This is due to a jitter issue. **Precision 60 hardware revision is not compatible with older software** New Precision 60 cameras will only work with TC7.3.3 and above software versions. If a user attempts to downgrade a codec connected to a newer Precision 60 camera to a version below TC7.3.3 the camera will not work as expected. This affects both the standalone Precision 60 cameras and the integrated cameras in MX700/MX800. Upgrading back to TC7.3.3 and above will resolve the issue. The new Precision 60 standalone camera can be identified by checking the P/N number underneath the camera base: 800-101373-02 For MX700/MX800 and SX80 the endpoint logs (all.log) will display: ERROR: Offered SW does not support this HW
Monitors / resolutions	**BugID: CSCtu99526** 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 causes 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. **VGA resolutions C40/C60** The Cisco TelePresence codec C40/C60 (rev. 1) will not provide proper analogue VGA output for any resolution of 1080 lines or more. **BugID: CSCuh68226** No video is displayed to share as content from a MacBook Air when using a MiniDisplay Port to VGA dongle, where a MacBook Pro has no issues displaying video as content. This is considered to be an Apple problem.
Authentication	**BugID: CSCtr32420** 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 passphrase on the unit.
Management	**Deleting the admin user** If the ‘admin’ user is deleted, 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. **TMS Upgrade** TMS versions earlier than 14.1 can upgrade to TC7.3, but not upgrade or downgrade a codec already running TC7.3 or newer. TMS 14.1 and later work with TC7.3.
IPv6	**BugID: CSCuo94615** Option 242 from DHCPv6 is not supported on TC endpoints.

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, X7.1, X7.2, X8.0 X.8.1, X.8.2, X8.5, X8.6, X8.7	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, 9.1.1, 9.1.2, 10.0, 10.5, 11.0* * 11.0 is supported from TC7.3.2	► Native registration. Encrypted calls are not supported in 8.6. ► 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: □ Convert IOS Gateway to SIP or MGCP. □ 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). ► 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). ► If dual stream (BFCP) does not work: □ Enable BFCP on SIP profile for endpoints in CUCM. □ Enable BFCP for SIP trunk profile if calling to/from a Cisco VCS. ► NTP: Configure Unicast NTP references for endpoints in CUCM. ► Provisioning: Make sure the endpoint has a DNS server that can resolve the host name, or change CUCM > System > Server, from hostname to IP address. ► CSCug19308: CUCM 8.6.2 directory returns more than the corporate limit set by the endpoint in the search. Fixed in CUCM 9.0. ► 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 call history instead of URI@domain. ► CAPF Authentication mode by authentication string is not supported if a Touch panel is not used. As a workaround, authentication string can be set in the web interface when the CUCM has requested it.
Cisco TelePresence System Video Communication Server (VCS)	X6.1, X7.0.1, X7.1, X7.2, X8, X8.1, X8.2, X8.5, X8.6, X8.7	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	IL1.1.5	**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 a 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, 2.2	
RadVision Gateway B40	5.6.0.0.4	

MCU interoperability

Equipment	Software version	Comments
Cisco TelePresence Server 7010	3.0, 3.1, 4.0, 4.1, 4.2,4.3	**CSCud79767**: Content from CUCM registered C series endpoints can take 10 seconds to arrive at TS. Fixed in TS2.42. **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 attempt 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 **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. **CSCuh38547**: Clearpath does not work correctly between TelePresence Server 3.1 and SX20, if SX20 is initiating the conference. Fixed in TC6.3.0.
Virtual TelePresence Server	3.1, 4.0, 4.1, 4.2,4.3	
Cisco TelePresence Server MSE 8710	3.0, 3.1, 4.0, 4.1, 4.2, 4.3	**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(3.67), 4.5(1.55)	
Cisco MCU 42xx	4.4 (3.67), 4.5(1.55)	
Cisco MCU 45xx	4.4(3.67), 4.5(1.55)	
Cisco CTMS	1.9	**NOTE:** We recommend customers to move to the TelePresence Server platform due to the number of caveats between the TC endpoints and CTMS, and the end-of-life of CTMS. ► **CSCul48235**: When a SX20 or MX300 G2 is in a call on CTMS and becomes the active speaker, the video quality is very poor for the first few seconds. This is not a problem on other endpoints, as they have a different decoder. ► When dialing to the CTMS, VCS cannot interwork the call (H.323 to SIP conversion). This conversion will make the call drop. ► Using a call-rate below 1152kbps results in CIF video in a CTMS conference. ► Endpoints that require the HD option key (SX20 and C20) and do not have it installed are not able to receive a presentation from CTS devices in CTMS conferences. ► **CSCuj13986**: TC endpoints (except EX60) without Premium Resolution option key do not display presentation sent from any CTS endpoint in a CTMS conference. ► TC interoperability must be enabled on the CTMS. ► Black Screen Codes are supported, but these will not work if the system is behind a firewall. ► **CSCud36845**: CTMS cannot handle a mid-call re-invite. This causes problems in mixed 720p/1080p environments ► **CSCum60110**: When the privacy shutter on the EX series camera is closed, it will stop sending video and the CTS detects this as packet loss and eventually disconnects the call/conference. Avoid closing the privacy shutter during a

		CTMS / CTS conference involving an EX series system. ► **CSCud45692**: CTMS does not respect the 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 starts transmitting this resolution, which the 720p endpoint cannot decode. ► Multisite is not supported for CTMS conferences.
Polycom RMX	7.8.0.246	Basic SIP/H.323 calls work. Encrypted calls: No audio on C/EX/MX/SX series (CSCuh50078), blocky video on SX20 (CSCuh32320) – both bugs are fixed in TC6.2.1. BFCP works.
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, S6.0, S6.1, S6.2,TCS7.0, TCS 7.1	

Endpoint Interoperability

Equipment	Software version	Protocol	Comments
Cisco TelePresence System 500series 3x00series 1x00series TX9000 TX9200 TX1310	1.10.7 (Ten Bears)	SIP	Encrypted calls are supported with TC6. **CSCtz95144**: TX9000 version earlier than 1.9.2 does not handle RTCP PLI on the BFCP channel, which results in no presentation. **CSCue55134** Point-to-point calls between MX200 and CTS endpoints. Video corruption can be observed 1 or 2 minutes into a call. The artifacts can be zebra pattern, color off, or blocky video that does not smooth out. Corruption clears up with I-frame. This may also cause high jitter value reports on the CTS side. Fixed in TC6.3. 720p30 is the maximum resolution for point-to-point calls. **CSCuw66608** CTS 3xxx and CTS13xx may in some situations show bad media quality from SX80 / MX700 / MX800 / MX800D (SIP Call) when the codec is running TC7.3.3 or TC7.3.4. A fix for this issue is targeted for TC7.3.5.

Cisco TelePresence System CTS500-32 TX1300 TX9000 TX9200	TX6.0.2 (Lago)	SIP	1080p30/60 support on Lago 1G codecs. Encrypted calls supported with TC6. **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. Bug is identified in TX software. **CSCue55134**: Point-to-point calls between MX200 and CTS endpoints. Video corruption can be observed 1 or 2 minutes into the call. The artifacts can be zebra pattern, color off, or blocky video that does not smooth out. Corruption clears up with I-frame. This may also cause high jitter value reports on the CTS side. **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.
Cisco TelePresence System MXP	F9.3	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/H.323	**CSCuj57861**: 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. **CSCus19470**: SX80 must disable H.265.

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

xAPI Changes

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

C series: http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-integrator-C Series/products-command-reference-list.html

SX series: http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/products-command-reference-list.html

Cisco TelePresence systems hardware dependencies

Due to occasional updates to hardware components there can be constraints to running older software on newly manufactured endpoints. To identify the endpoints compatibility level, you can access the web interface of the endpoint and click on Configuration > System Status > SystemUnit. Scroll down to the compatibility level on this page. You can also find the compatibility level using the xAPI to execute the command *xStatus SystemUnit Hardware Module CompatibilityLevel.*

The below tables can be used to identify software constraints based on the compatibility level of your endpoint.

Downgrading to an unsupported software version will fail.

The latest software releases are always backward compatible with all hardware versions.

Examples of executing the API command:

xStatus SystemUnit Hardware Module CompatibilityLevel

System	Output	Minimum version
SX10	*s SystemUnit Hardware Module CompatibilityLevel: “2”	7.3.2
SX20	*s SystemUnit Hardware Module CompatibilityLevel: “4”	7.2.1
C40	*s SystemUnit Hardware Module CompatibilityLevel: “0”	No software constraints

Compatibility level and software constraints

C Series, MX200 G1, MX300 G1, Profile Series and EX Series

Compatibility level	Applicable systems	Description	Minimum software version		
			TC5[1)]	TC6	TC7
0	All	N/A	All	All	All
1	All	N/A	All	All	All
2	EX/MX	N/A	5.1.6	All	All
2	C20	N/A	5.1.1	All	All
3	C40	N/A	5.1.5	All	All
V	MX300	N/A	5.0.1	All	All
1V	MX300	N/A	5.1.0	All	All
2V	MX300	N/A	5.1.6	All	All

4	All	N/A	5.1.11	6.2.2/ 6.3.0	All

[1)] TC5 will shortly be end of support; customers should migrate to TC7.

SX20, MX200 G2, MX300 G2

Compatibility level	Applicable systems	Description	Minimum software version		
			TC5[1)]	TC6	TC7
2	SX20	N/A	5.1.0	All	All
3	SX20	N/A	5.1.6	All	All
4	SX20	N/A	None		7.2.1
0	MX200 G2	N/A	None	None	7.1.0
1	MX200 G2	N/A	None	None	7.3.0
0	MX300 G2	N/A	None	None	7.0.0
1	MX300 G2	N/A	None	None	7.3.0

1) TC5 will shortly be end of support; customers should migrate to TC7.

SX80, MX700 and MX800 / MX800 Dual

Compatibility level	Applicable systems	Description	Minimum software version
			TC7
0	SX80	N/A	TC7.1.0
0	MX700/MX800	N/A	TC7.1.2
0	MX800 Dual	N/A	TC7.3.2

SX10

Compatibility level	Applicable systems	Description	Minimum software version
			TC7
0	SX10	N/A	~~TC7.1.0~~ TC7.2.0
1	SX10	N/A	TC7.2.0
2	SX10	N/A	TC7.3.2

Identify compatibility level using the hardware TAN number

You can identify software dependencies by looking at the TAN number located on a sticker on the system. Find the compatibility level from the TAN number in the tables below, and look up the software dependencies in the above table.

EX series and MX G1 series

System	TAN number	Compatibility level
EX60		
	800-35326-05	0
	800-35326-06	1
	800-35326-07	1
	800-35326-08	2
(new LCD)	800-35326-09	2
(new LCD)	800-35326-10	4
Non-crypto	800-36052-05	0
Non-crypto	800-36052-06	1
Non-crypto	800-36052-07	1
Non-crypto	800-36052-08	2
Non-crypto (new LCD)	800-36052-09	2
Non-crypto (new LCD)	800-36052-10	4
EX90		
	800-35448-05	0
	800-35448-06	1
	800-35448-(07-10)	2
	800-35448-11	4
(New LCD)	800-35448-12	4
Non-crypto	800-36051-05	0
Non-crypto	800-36051-06	1
Non-crypto	800-36051-(07-10)	2
Non-crypto	800-35448-11	2
Non-crypto (New LCD)	800-35448-12	4
MX200		
	800-36834-02	0

	800-36834-03	1
	800-36834-05	2
	800-36834-06	4
Non-crypto	800-37182-02	0
Non-crypto	800-37182-03	1
Non-crypto	800-37182-05	2
Non-crypto	800-37182-06	4
MX300		
	800-36919-03	V
	800-36919-04	2V
	800-36919-05	4V
Non-crypto	800-37822-03	V
Non-crypto	800-37822-04	2V
Non-crypto	800-37822-05	4V

C series

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

	800-35367-02	1
	800-35367-04	4
Non-crypto	800-36048-01	0
Non-crypto	800-36048-02	1
Non-crypto	800-36048-04	4
C90		
	800-35342-02	0
	800-35342-03	1
	800-35342-04	4
Non-crypto	800-36049-02	0
Non-crypto	800-36049-03	1
Non-crypto	800-36049-04	4
SX20	TAN number	Compatibility level
	800-36554-01	2
	800-36554-02	3

Cisco TelePresence Touch 8 hardware dependencies

New hardware revisions for Cisco TelePresence Touch 8

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	HW level	System type	Minimum release		
			TC5[1)]	TC6	TC7
800-35447-04	0	EX	All	All	All
800-35343-05	0	SX20/C/Profile	All	All	All
74-9543-02	0	MX	All	All	All
800-35447-06	1	EX	5.1.4	All	All
800-35343-07	1	SX20/C/Profile	5.1.4	All	All
74-9543-04	1	MX	5.1.4	All	All
800-38887-01	2	EX	5.1.4	All	All
800-38886-01	2	MX	5.1.4	All	All
800-38885-01	2	SX20/C/Profile	5.1.4	All	All
800-38887-02	3	EX	5.1.4	All	All
800-38886-02	3	MX	5.1.4	All	All
800-38885-02	3	SX20/C/Profile	5.1.4	All	All

[1)] TC5 will shortly be end of support; customers should migrate to TC7.

Cisco TelePresence Touch 10 hardware dependencies

New hardware revisions for Cisco TelePresence Touch 10

Systems that currently support Touch 10 are SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800 and MX800D.

The hardware revision number will be displayed on the touch panel during boot in the lower right corner on the touch screen.

Hardware revision	Applicable systems	Description	Minimum software version
			TC7
102300-3 102310-0	SX80 MX200 G2 MX300 G2 MX700 MX800 MX800D	N/A	All supported codec software versions are compatible
	SX10 SX20	N/A	TC7.2.0
102310-1	All	N/A	TC7.2.1

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	http://www.cisco.com
Cisco Software Download	http://www.cisco.com/cisco/software/navigator.html
Cisco TelePresence User Documentation	http://www.cisco.com/go/TelePresence/docs

Software filenames

The correct software filenames are listed in the following table.

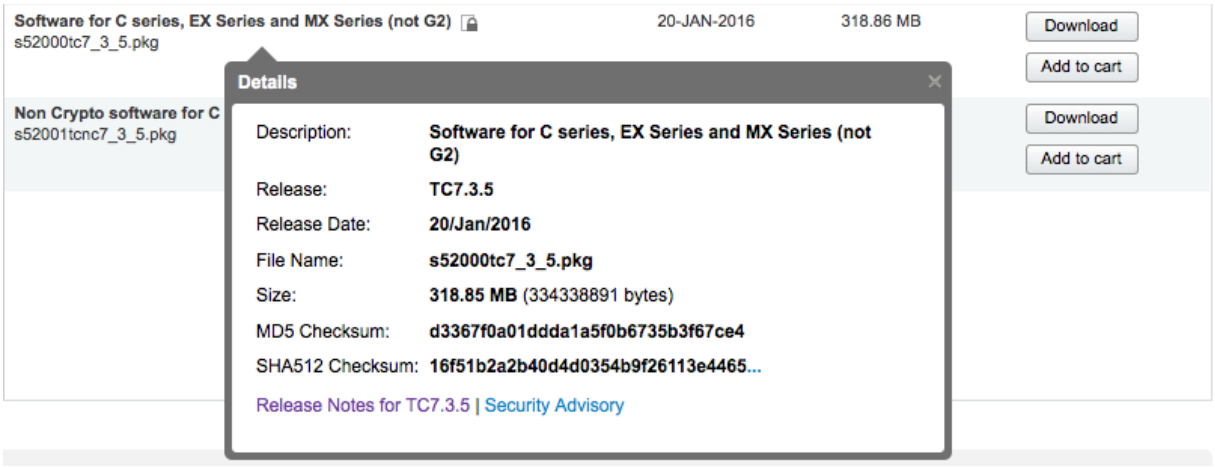
Cisco TC system	Software for EX Series, C Series, MX200 G1	Software for SX20	Serial number range
AES Encryption	s52000tc7_3_6.pkg	s52010tc7_3_6.pkg	All
No Encryption	s52001tcnc7_3_6.pkg	s52011tcnc7_3_6.pkg	All
AES Encryption for CUCM	cmterm-s52000tc7_3_6.k3.cop.sgn	cmterm-s52010tc7_3_6.k3.cop.sgn	All
No Encryption for CUCM	cmterm-s52001tcnc7_3_6.k3.cop.sgn	cmterm-s52011tcnc7_3_6.k3.cop.sgn	All

Cisco TC system	Software for SX10	Software for MX200 G2, MX300 G2	Software for SX80, MX700, MX800	Serial number range
Encryption and Non-encryption*	s52030tc7_3_6.pkg	s52010tc7_3_6.pkg	s52020tc7_3_6.pkg	All
Encryption and Non-encryption* for CUCM	cmterm-52030tc7_3_6.k3.cop.sgn	cmterm-s52010tc7_3_6.k3.cop.sgn	cmterm-s52020tc7_3_6.k3.cop.sgn	All

*SX10, SX80, MX700, MX800, MX200 G2 and MX300 G2 do not have separate software packages for crypto and non-crypto. These systems require a crypto option key to enable crypto algorithms.

Software integrity verification

To verify the integrity of the software image you have downloaded from cisco.com you can calculate a SHA512 checksum and verify that it matches with the one listed on the software download page. To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

To calculate a SHA512 checksum on your local desktop please see the table below.

Operative system	SHA512 checksum calculation command examples
Microsoft Windows	Open a command line window and type the following command > certutil.exe -hashfile s52000tc7_3_6.pkg SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 s52000tc7_3_6.pkg

Linux	Open a terminal window and type the following command
	$ sha512sum s52000tc7_3_6.pkg
	Or
	$ shasum -a 512 s52000tc7_3_6.pkg

If the SHA512 checksum matches you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

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.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)