Cisco TelePresence

SX and MX Series

Collaboration Endpoint Software 8

D15314.04

May 2016

Contents

Document revision history

Revision	Date	Description
04	May 4th 2016	Release of CE 8.1.1, minor release with fix for bug CSCuz26935
03	April 8th 2016	Release of Collaboration Endpoint Software 8.1.0
02	January 20th 2016	Release of CE8.0.1, minor release with fix for bug CSCux85199
01	November 25th 2015	Release of Collaboration Endpoint Software 8.0.0

Introduction to Collaboration Endpoint Software 8

This release note describes the features and capabilities included in the Cisco TelePresence MX200 G2, MX300 G2, MX700, MX800, MX800 Dual, SX10, SX20 and SX80 Collaboration Endpoint Software version 8. Collaboration Endpoint Software is only supported by the endpoints listed above.

The Collaboration Endpoint software version 8 can be downloaded from http://www.cisco.com.

Important notes and warnings for this software version

Before upgrading from TC software to Collaboration Endpoint Software it is important to check that your environment supports the changes. We recommend that you read the release note thoroughly before upgrading.

Equipment and feature considerations before upgrading from TC to Collaboration Endpoint Software 8.x

The following features and equipment is not supported with Collaboration Endpoint Software:

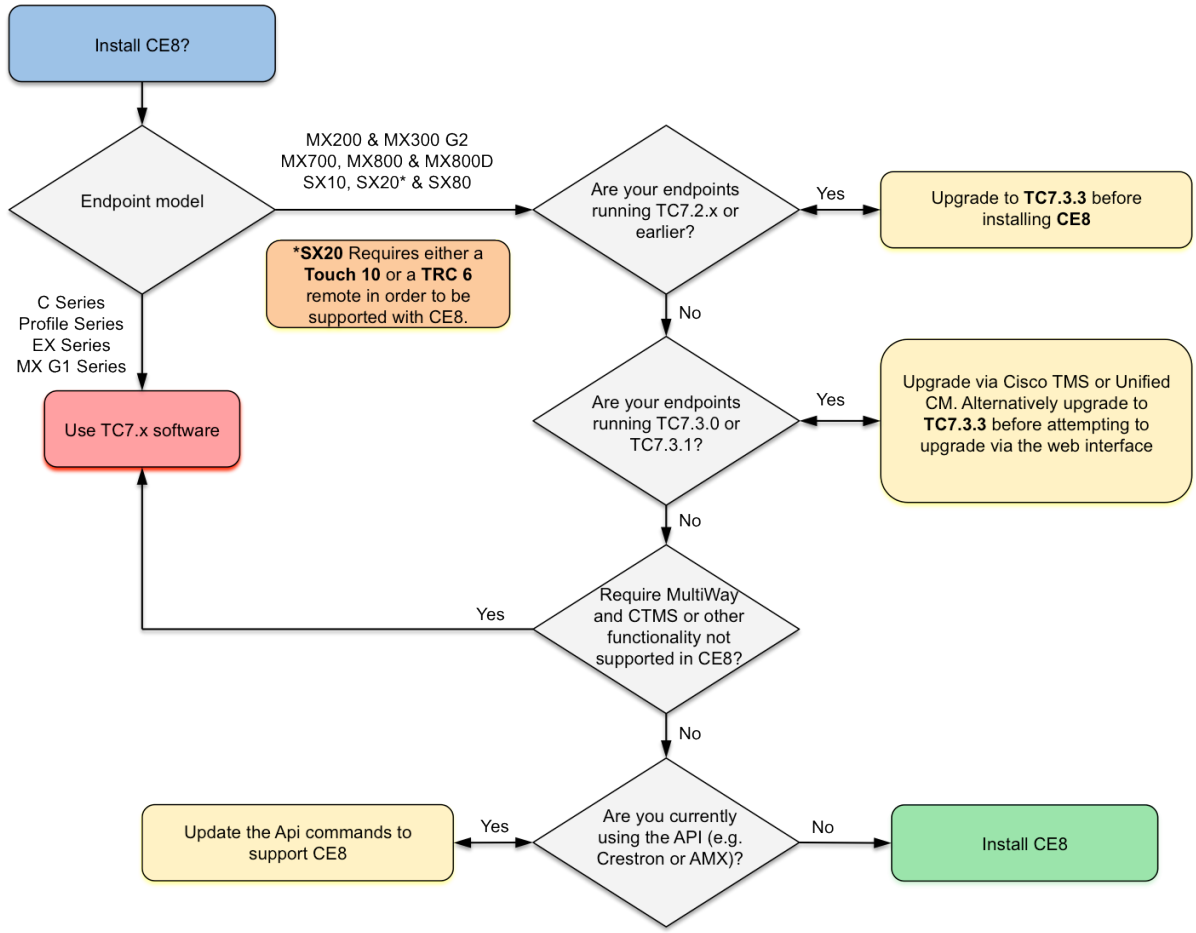
- Cisco TelePresence Touch 8
  - Replaced by the Cisco TelePresence Touch 10
- Cisco TRC5 remote control and below
  - Replaced by the Cisco TRC6 remote for systems that support remote control as a control device i.e. SX20 and SX10
- Multiway
  - Replaced by ad-hoc conferencing (requires CUCM MediaResourceGroupList)
- CTMS (TIP/MUX)
  - Replaced by other multipoint conferencing solutions involving Cisco TelePresence Server (virtual and appliance), Cisco TelePresence MCU and Cisco TelePresence Conductor
- Medianet (affects Prime Collaboration Manager monitoring)
- TC Console
  - Replaced by "CE Console" (audio only)

Note: Minor discontinuations that are not deemed as significantly relevant are not listed here. Please refer to the API guide for changes.

Upgrading from TC to Collaboration Endpoint Software

Upgrading systems from TC software to Collaboration Endpoint software is supported for all the endpoints in the new endpoint portfolio.

The diagram below should be used as an example of eligibility verification only, as there might be other environmental factors that need to be considered before upgrading.



Cisco TelePresence SX20 Quick Set that utilizes either a Touch 8 or TRC5 remote control should not be upgraded to Collaboration Endpoint SW. Touch 10 or TRC6 remote control is required to operate endpoints using Collaboration Endpoint SW.

CE8.1.0 - Discontinued support for TLS 1.0

Cisco TelePresence Endpoints running CE8.1.0 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 endpoint is upgraded to CE8.1.0. Make sure TLS 1.2 or 1.1 is enabled on the server before upgrading to CE8.1.0. Older browsers may not be able to reach the endpoint's web interface on HTTPS if the browser only supports TLS 1.0.

CE8.0.0 - Updated CA certificates for Collaboration Edge

Note: Only applies when upgrading from TC7.3.2 and earlier to CE8.0.0.

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.

Note well before upgrading

- Collaboration Endpoint Software is not supported by the legacy Cisco TelePresence portfolio, which includes the C Series, Profile Series, EX Series and MX G1 Series.
- Collaboration Endpoint Software inherits fundamentals from TC software but should be considered as new software and not as continuation of TC software.
- We highly recommend upgrading endpoints to TC7.3.3 or above before proceeding with the upgrade to Collaboration Endpoint Software.
- Upgrading to Collaboration Endpoint Software from TC7.3.0 and TC7.3.1 is not supported via the web interface. These software versions have been deferred from cisco.com and are no longer available. Upgrading from these software versions via TMS or CUCM will work.
- Cisco TelePresence SX20 Quick Set requires either a Touch 10 or a TRC6 remote control in order to be supported with Collaboration Endpoint Software.
- Attempts to pair a Touch 8 to a codec running Collaboration Endpoint Software results in an on-screen warning message that the specific touch controller is not supported.
- Attempts to use the TRC5 with a codec running Collaboration Endpoint Software results in an on-screen warning when an unsupported command is received.
- Endpoints running CE8.0.0 requires TMS 15.0 or later, the latest version is always recommended to ensure compatibility.

Downgrading from Collaboration Endpoint Software to TC

Downgrading from Collaboration Endpoint Software to TC software is supported. When downgrading a system paired with a Touch 10 panel from TC to Collaboration Endpoint Software, the Touch 10 panel will be downgraded automatically. We recommend first downgrading from CE8 to TC7.3.3 or later before downgrading further.

Collaboration Endpoint Software 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 Collaboration Endpoint Software 8 (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-s52010ce8_0_0.**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

Camera firmware

In the table below you can find an overview of the camera software included in the CE software release. Only new camera software is listed. If not listed, the camera software is the same as on the previous release.

Release	Hardware name/ID	Software name/ID	Notes
CE8.1.1	Precision 60 55000000	HC8.1.1.a8488eee	
CE8.1.0	Precision 60 55000000	HC8.1.0.b8c0ca3	
CE8.0.1	N/A	N/A	
CE8.0.0	PrecisionHD 1080p 4x 52000000	S01752-2.0 FINAL ID:20011	
	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC12 ID:20035	
	PrecisionHD 1080p 4x S2 53000000	S01777-2.2 RC12 ID:20035	
	PrecisionHD 1080p 12x 5000000(1-4)	S01718-4.0 FINAL ID:40084	
	Precision 60 55000000	HC8.0.0.2272c42	

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.

Deferred software versions

A software version is deferred when we find critical 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.

CE8.0.0, CE8.0.1, CE8.1.0 deferral for all platforms

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/ce8/release-notes/cisco-ce800-ce801-ce810-deferral-notice.pdf

CE8.0.0 deferral for SX20

Deferred 20th of January 2016.

Please read the deferral notice for more information.

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

New features and functionality in CE8.1.1

- This is a minor release and contains a bug fix for CSCuz26935 only

New feature and functionality descriptions CE8.1.1

CE8.1.1 fixes critical security bug CSCuz26935 (CVE-2016-1387)

A 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 on the vulnerability, please refer to the security advisory: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160504-tpxml

The following vulnerable CE8 releases has been deferred from Cisco.com for all platforms:

CE8.0.0, CE8.0.1 and CE8.1.0

More details 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-ce801-ce810-deferral-notice.pdf

Cisco recommends all peers that are currently running one of the above software versions to upgrade to CE8.1.1 where this issue is resolved.

New features and functionality in CE8.1.0

- Cisco Spark activation for Cisco TelePresence SX10 Quick Set (CTS-SX10N-K9)
- New visual design
- In-Room Control
- PresenterTrack
- Intelligent Proximity updates
  - Sharing of mouse pointer
  - Enable / Disable Intelligent Proximity services on-screen
- Direct sharing of presentation to far end
- Minor changes
  - On-screen overscan adjustments
  - Support for encrypted active control signaling
  - Audio avatar removed in MultiSite and point-to-point calls

New feature and functionality descriptions CE8.1.0

Cisco Spark activation for Cisco TelePresence SX10 Quick Set (CTS-SX10N-K9)

Collaboration Endpoint Software 8.1.0 introduces support for Cisco Spark activation. This will register the supported endpoint in the Spark Cloud and can be used for video calls without the need for additional TelePresence infrastructure. The only Room System that supports Cisco Spark registration with CE8.1.0 is the Cisco TelePresence SX10 Quick Set with PID number **CTS-SX10N-K9**. This hardware revision has a built-in ultrasound emitter in the front panel to allow pairing with a mobile Cisco Spark client. Older revisions of the SX10 are not supported for Cisco Spark activation as they do not have the required ultrasound emitter and do not provide Cisco Spark as an activation alternative.

Requirements for activating your Room System on Cisco Spark

In order to activate a SX10 on Cisco Spark the following requirements must be fulfilled:

- Cisco TelePresence SX10 Quick Set with the correct PID (CTS-SX10N-K9)
  - You can find the PID on the back of the unit
- Running software is Collaboration Endpoint Software 8.1.0 or later
- Encryption option key installed (this is installed by default)
  - If the Encryption option key is not installed, you can contact Cisco Licensing and they will provide this key for free
  - If this key is not installed, you will not be given the option to activate the endpoint on Cisco Spark during the setup
- TRC 6 remote control
  - Touch 10 is currently not supported when the Room System is registered to Cisco Spark
- A Cisco Spark activation code acquired from https://admin.ciscospark.com
  - Requires a paid subscription for your organization
  - Please contact your Cisco Sales representative for more information

On-boarding to Cisco Spark

On the first time setup wizard you are asked if you want to activate your Room System on Cisco Spark or on an existing on-premise infrastructure. After selecting the Cisco Spark activation you must type in the required activation code and press the activate button on screen.

When the room system is activated on Cisco Spark, it downloads the newest version of Spark Room OS that looks similar to the Collaboration Endpoint Software user interface.

Spark Room OS does not have the same management capabilities as Collaboration Endpoint Software as access to the API and web interface is restricted. Only a few simple configuration options is available in the OSD UI. From this point the Room System is managed by Cisco and if there are any issues, contact Cisco Technical Assistance center through the Cisco Spark Mobile application or through the Cisco Cloud Collaboration Management (https://admin.ciscospark.com).

For more information on the Spark Room OS and its features see:

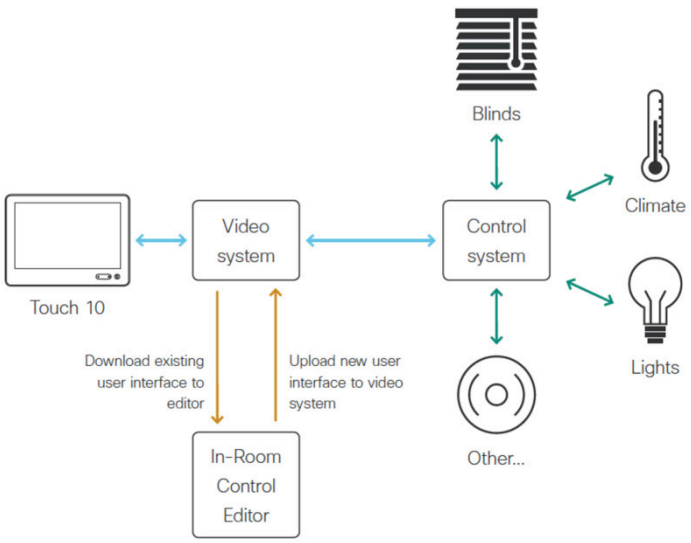
https://help.webex.com

New visual design

The user interface has been updated with a new visual design. This includes both the on-screen user interface when the endpoint is operated using a TRC 6 remote control and on the Touch 10. Labels and icons have a new look in MultiSite and Multistream calls.

In-Room Control

With the In-Room control feature you can customize the Touch 10 user interface to allow control of peripherals in your meeting room, for example lights and blinds. A third-party control system with hardware drivers for the peripherals, for example Crestron, AMX, Apple HomeKit, or Android is required to control the peripherals.



The graphical user interface can be designed by anyone, using the simple drag and drop GUI editor available on the endpoint's web interface. The editor can also be downloaded from the codec and used offline to later upload the design from a file.

For more information about setting up the In-Room control feature, refer to the user guide: http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce81/sx-mx-in-room-control-guide-ce81.pdf

PresenterTrack

PresenterTrack is a feature that enables one of the cameras in a SpeakerTrack 60 or Precision 60 camera to digitally track a presenter/instructor within an overview image on a stage or in a room. This allows the presenter to walk freely within the tracking area while the camera is tracking the presenter. Note that the camera will not physically follow the presenter as the tracking is done digitally.

The feature is configured from the endpoint's web interface. We recommend being present in the room while the feature is configured. The feature is configured by selecting a trigger zone in the configuration wizard; an area within the overview image that activates PresenterTrack when a face is detected. Once the trigger zone has been selected the feature can be activated and deactivated from the Touch 10.

Note: The PresenterTrack feature is only available from CE8.1.0 and requires a SpeakerTrack 60 or Precision 60 camera. The SpeakerTrack and PresenterTrack feature will not be active at the same time unless the endpoint is configured for "Briefing Room" mode.

Intelligent Proximity updates

Sharing of mouse pointer

With the Cisco Proximity for Desktop 1.1.0 or later the application renders the mouse pointer. Note that this effect is also present in CE8.0.0 with the new app version.

Enable and disable Intelligent Proximity services on-screen

When operating an endpoint using the TRC 6 remote control, a user can temporarily enable and disable the Intelligent Proximity services. This functionality was in previous releases of CE only available on the Touch 10.

Direct sharing of presentation to far-end

The endpoint can be configured to automatically share presentations to the far-end participants when connecting a presentation source while in a call. This requires no further interaction from the user when connecting the presentation source. When connecting the presentation source outside of a call, the configuration acts like the "OnConnect" configuration and automatically displays the presentation locally. If a presentation source is already connected and the user makes a call, the presentation must be shared manually, or re-connected.

Minor changes

This section covers a set of relevant minor changes introduced in Collaboration Endpoint Software 8.1.0.

On-screen overscan adjustments

This feature is for adjusting the image to fit the screen in scenarios where parts of the image are not visible. Most screens have built-in settings to adjust the image and these should be attempted first. For systems that are operated with a TRC 6 remote control you can adjust the overscan values on the setup wizard, or from the settings menu by selecting "Screen Adjustments".

Support for encrypted active control signaling

Collaboration Endpoint Software version 8.1.0 adds support for encrypted Active Control signaling.

Audio avatar removed in MultiSite and point-to-point calls

The full screen avatar that previously represented an audio participant has been removed in point-to-point and MultiSite calls. The avatar may still be displayed in bridged calls; the endpoint does not control over the audio avatar in these scenarios.

New features and functionality in CE8.0.1

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

New feature and functionality descriptions CE8.0.1

CE8.0.1 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 CE8.0.1 release.

New features and functionality in CE8.0.0

- Cisco Intelligent Proximity
  - Cisco Intelligent Proximity with PC and MAC clients
- Multistream
- Microphone LED behavior changes
- Advanced Settings on-screen authentication
- SX20 Quick Set user interface is aligned with SX10 Quick Set when used with TRC6
- Supported resolutions
- 1080p presentation resolution on SX10 Quick Set
- Minor changes
  - DHCP option 150 is always requested
  - Measure ultrasound-pairing quality using the VU meter
  - Provision endpoints to use HTTPS only from CUCM
  - Snap to Whiteboard improvements

New feature and functionality descriptions CE8.0.0

Cisco Intelligent Proximity

The Cisco Intelligent Proximity feature is supported in CE8.0.0 and all endpoints that support this software version are capable of utilizing this feature. Please see below for maximum endpoint to Proximity connections per endpoint. Please note that these values include both connected laptop and mobile devices in total.

Endpoint	Maximum simultaneous Proximity connections
SX10	7
SX20	7
SX80	10
MX200 G2 MX300 G2	7
MX700 MX800 MX800D	10

Note: Cisco Proximity currently requires the device that is connecting to the endpoint to have an IPv4 routable network path to the endpoint on port 443 (HTTPS). HTTPS must be enabled on the endpoint.

Note: The endpoint requires a speaker system that is capable of producing ultrasound to allow wireless pairing with devices running the Cisco Proximity client application.

The Intelligent Proximity feature allows the users to connect their PC / MAC, iOS or Android device to an endpoint wirelessly. Depending on what services has been enabled for Intelligent Proximity, the user can get locally or remotely shared content to their Android or iOS device, and/or access endpoint call control. When Intelligent Proximity is connected with the Cisco Proximity app for PC or MAC, the user can wirelessly share images of their laptop screen locally if the system is not in a call and remotely if the system is in a call.

The following three Intelligent Proximity services can be enabled and disabled separately on the endpoint by the administrator.

First ensure the endpoint has Proximity Mode is set to "On" to enable basic device pairing and enable one or more of the following Intelligent Proximity services to get started.

- Content share to clients
    - When enabled, this feature allows a user to receive content that is being shared locally or remotely to their iOS or Android device.
    - The endpoint saves up to 10 content snapshots and sends these to any connected device. This is useful if a participant wants to review a previous snapshot. The user will be able to save the content to their handheld device to view it later. These snapshots are deleted on the endpoint when the call is disconnected. Note that snapshots are not deleted from the paired device in a call disconnect event.
- Content share from clients
    - When enabled this feature allows PC and MAC clients to share content snapshots locally and remotely when in a call.
    - When screen sharing is enabled from the PC / MAC Proximity application while in a call, a remote presentation will automatically be triggered and the shared content is visible to all participants
- Call control
    - When enabled this feature allows users connected to Intelligent Proximity via their iOS or Android device to perform basic call control actions.
        - Directory lookups
        - Dial / End call / Mute / DTMF tones / Add participants / Volume control

If Proximity Mode is enabled and one or more of the Intelligent Proximity services is enabled, the Intelligent Proximity icon will show on the Touch 10 panel in the top left corner. By pressing this icon, Intelligent Proximity services can be disabled and enabled on demand. This is useful if a user wants to have Intelligent Proximity services disabled during a particular session.

Cisco Intelligent Proximity pairing mode is enabled by default on our complete room systems (MX series) and all Intelligent Proximity services are disabled by default. This means that the user is able to pair with the system out of the box, and gets a notification that the services are not enabled.

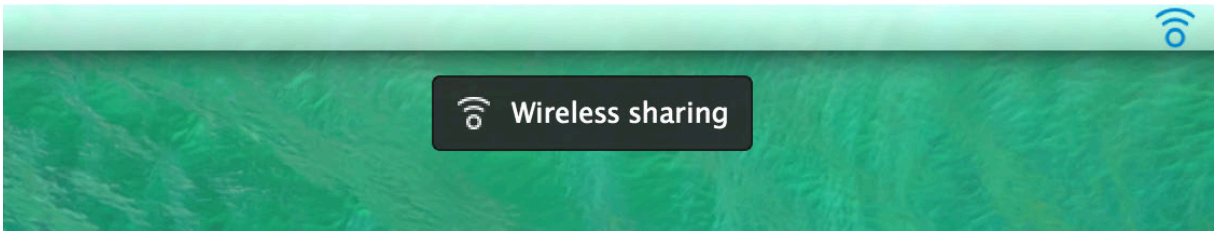
The integrator systems (SX series) have Cisco Intelligent Proximity pairing mode disabled by default, because we cannot account for how these devices are being setup together with third party equipment. Intelligent Proximity pairing mode must be enabled manually for the SX series.

Note: Please visit the Proximity community at the link below for support, inquiries and troubleshooting information. https://www.cisco.com/go/proximity-support

Content sharing from PC and MAC clients to endpoint via Cisco Proximity

Collaboration Endpoint Software introduces Intelligent Proximity pairing and content sharing capability for PC and MAC clients running the Cisco Proximity application. The Cisco Proximity application for PC is released as beta.

Images are sent to the endpoint as snapshots of the screen at low frame rate. This makes the functionality ideal for presenting still images, such as slide-based content, but it does not work well for content in motion, for example video. When content is shared via Proximity, a sticky "Wireless sharing" notification will be displayed on-screen.



This is displayed to avoid unintended sharing of content, and to confirm that the content is shared via Proximity.

The Cisco Proximity application will only share visual content and not audible content.

Please read the Cisco Proximity Desktop release notes for more information: https://www.cisco.com/go/proximity-support.

Cisco Proximity application availability and requirements

Application	Minimum requirements	Release notes	Where to download
Cisco Proximity for iOS	iOS 7 and above	Apple App Store	Apple App Store
Cisco Proximity for Android	Android 4.0 and above	Google Play Store	Google Play Store
Cisco Proximity MAC client	OSX 10.9 (Mavericks) and above	https://www.cisco.com/go/proximity-support https://proximity.cisco.com/changelog.html	https://proximity.cisco.com
Cisco Proximity PC client (Beta)	Windows 7 and above	https://www.cisco.com/go/proximity-support https://proximity.cisco.com/changelog.html	https://proximity.cisco.com

The Cisco Proximity desktop applications will auto update when a new version is available.

Note: The Cisco Proximity Client for PC (Windows) is currently in beta.

Note: Cisco Technical Assistance Center (TAC) does not provide support for the Cisco Proximity applications for PC, MAC, Android and iOS devices, as they are free of charge.

Any issues and bug reports linked to the client applications should be posted in the Cisco Support Forums. Cisco representatives are following up the Cisco Proximity community. Inquiries about the Intelligent Proximity feature on the endpoint are also applicable.

Please follow this link for support and issue reports: https://www.cisco.com/go/proximity-support

Multistream

Multistream is a feature that enables the endpoint to send and receive multiple streams of video at different resolutions. This takes down transcoding load on the TelePresence Server and lets the endpoint use lower quality streams for smaller resolution images depending on the layout selected on the endpoint. Audio and presentation are still transcoded by the Multistream enabled TelePresence Server.

This feature will enhance the user experience while in a conference with multiple participants. The main benefits of this feature are:

- A two-screen system i.e. Cisco TelePresence MX700 and MX800 Dual, will be able to utilize both screens for video participants when participating in a Multistream enabled conference.
- Layout control is more flexible and can be selected on the endpoint locally. This experience is enhanced when using a two-screen system.

The above example shows a two-screen system in a conference where Multistream is not enabled. The endpoint is receiving only one transcoded stream from the Cisco TelePresence Server.

The above example shows the same conference with Multistream enabled.

When connecting a third screen on SX80, MX700, MX800 and MX800 Dual systems or a second screen to MX200 G2, MX300 G2 and SX20 systems, the additional screen is reserved for presentation only and will not display video participants in a Multistream enabled conference.

If Multistream is enabled on the endpoint it will automatically use Multistream whenever possible in a conference that supports Multistream. If Multistream is not available in the conference it will fall back to transcoding. The same might happen if the bandwidth is too low or if the endpoint is experiencing

excessive packet loss. To enable Multistream after a fallback to transcoding the endpoint must end the call and dial back into the conference.

Note: Multistream is disabled by default on the endpoint.

Note: Multistream requires all required video infrastructure and endpoints to be on the latest available software.
Note: Bandwidth recommendation for Multistream systems with single screen is 4 Mbps. For systems with dual screens the bandwidth recommendation is 6 Mbps.

Note: Multistream is currently not supported on SX10. Please see the "Known issues" section in this document for more information.

Microphone LED behavior changes

After upgrading to Collaboration Endpoint Software the LED surrounding the microphone mute button on the external microphones and the Cisco TelePresence Touch 10 panel will not glow unless the system is in, receiving or making a call. Previous behavior of this LED has been a constant glow of green or red color where green indicates that the microphones are active and red indicates that the microphones are muted even if the system was not in a call.

The microphone LED will glow and the mute button becomes active in the following scenarios:

- When initiating an outgoing call and until the call is disconnected.
- When receiving an incoming call and until the call is disconnected.
- When activating the VU meter on the web interface to test the audio levels.

The color indications, green for active and red for muted have not changed.

Note: The Cisco TelePresence SX20 Quick Set with PID number CTS-SX20CODEC will not have this functionality and the microphone LED will still be lit when the system is idle. For SX20 Quick Set with PID number CTS-SX20NCODEC the microphone LED behavior is aligned with the description above. The PID number is located on the bottom side of the codec.

Advanced Settings on-screen authentication

The Advanced Settings on the Touch 10 panel is protected with the admin credentials.

The on-screen Advanced Settings for SX10 and SX20 can be PIN protected to prevent unauthorized users from changing the endpoint's configurations. This configuration can be set using the codec web interface.

SX20 Quick Set user interface is aligned with SX10 Quick Set when used with TRC6

The SX20 Quick Set and SX10 Quick Set support endpoint control with the TRC6 remote. The SX20 Quick Set on-screen user interface is aligned to match the interactive SX10 Quick Set user interface on Collaboration Endpoint Software.

Supported resolutions

The SX80, MX700, MX800 and MX800D have added support for WUXGA (1920x1200) both locally and in call.

Collaboration Endpoint Software only supports 16:9 or 16:10 resolutions. This is valid for all endpoints that have Collaboration Endpoint Software installed.

1080p presentation resolution on SX10 Quick Set

A software enhancement is added for SX10 Quick Set to allow sharing 1080p presentations locally and in a call at 5 frames per second.

Minor changes

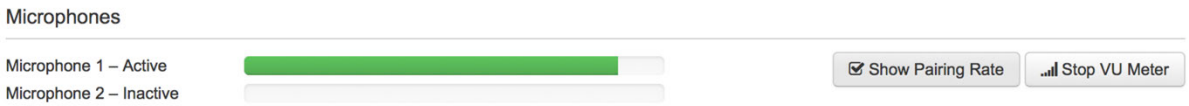
This section will cover a set of relevant minor changes introduced in Collaboration Endpoint Software 8.0.0.

DHCP Option 150 is always requested

Endpoints will always use option 150 in the DHCP request. This is not configurable.

Measure ultrasound-pairing quality using the VU meter

VU meter is a web tool to verify microphone audio levels. This tool provides a way to confirm that ultrasound is correctly played out from the endpoint's speaker(s) and picked up by the endpoint microphone(s). To enable this function, start the VU meter from the endpoint web interface (Configuration - Peripherals - VU Meter) and check the "Show Pairing Rate" button. Scaling from 0-100% the green bar indicates how well the endpoint can decode the ultrasound signals that the endpoint itself is sending out.



Provision endpoints to use HTTPS only from CUCM

Endpoints can be provisioned from CUCM to use HTTPS only or HTTPS+HTTP.

Snap to Whiteboard improvements

The "Snap to whiteboard" feature has been improved. If the system detects a presenter standing next to the whiteboard, it will now automatically expand the image to include the presenter. If you have previously used this feature in TC7.3.x, we recommend that you in CE8.0.0 re-configure the whiteboard preset to fully enable this feature. Please read the SX80 administrator guide for more information.

Open and resolved caveats in CE8

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. **No subset of open or resolved bugs will be listed in the release notes**. A pre-defined link will provide the correct list of all 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 Collaboration Endpoint Software.

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'.

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

Software version	Resolved caveats	Open caveats
CE8.1.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.1&sb=fr&sts=fd&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8&sb=anfr&sts=open&srtBy=byRel&bt=custV
CE8.1.0	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.0&sb=fr&sts=fd&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.0&sb=anfr&sts=open&srtBy=byRel&bt=custV
CE8.0.1	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.1&sb=fr&sts=fd&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.1&sb=anfr&sts=open&srtBy=byRel&bt=custV
CE8.0.0	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.0&sb=fr&sts=fd&srtBy=byRel&bt=custV	https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.0&sb=anfr&sts=open&srtBy=byRel&bt=custV

Known limitations

Limitations

Equipment / Feature	Summary
CUCM	**H.323 and SIP consideration when provisioned by CUCM** 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. When CUCM provisioning is active, H.323 mode is disabled. We recommend TelePresence customers to migrate from H.323 to SIP.
SX20 Quick Set	**Microphone mute button** It is a known issue that the SX20 Quick Set with PID CTS-SX20CODEC microphone mute button is still lit (red or green) when the system is not in a call. This is resolved in newer hardware revisions of the SX20 Quick Set with PID CTS-SX20N-CODE running CE8. The PID number is located on the bottom side of the codec. **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*
SX10 Quick Set	**H.323** H.323 is not supported on this endpoint.
SX80, MX700, MX800, MX800D	**Bandwidth limitation** The maximum available bandwidth for these systems is limited to 6000 kbps (previously 10000 kbps) due to a limitation related to high load on the endpoints. A fix for this is planned for a future release.

TRC6 remote control	**Hold button** Hold button is supported when the system is paired to a Touch 10, but not when using the TRC6 remote control with SX10 Quick Set or SX20 Quick Set.
H.265	**H.265 will only work with SIP** The H.265 protocol will only work with SIP and is currently only supported with SX80/MX700/MX800/MX800D.
Multistream	**Bug ID: CSCut47719** Endpoints operating in Multistream mode do not render messages received via Active Control. For example, users in Multistream mode will not see warning messages about the conference end time. **Multistream SIP SDP message size can be too large for CUCM** The symptom is that the call is failing. CUCM version < 11.0 SU1 has a default SIP Max incoming message size of 11000 bytes (also includes upgrades to CUCM 11.0). This setting has to be manually changed to 15000 bytes to be able to process incoming SIP messages containing Multistream negotiation. This change requires a restart of the CUCM service. Cisco recommends CUCM 11.0 SU1 for Multistream. **Allow iX application media is required in CUCM SIP Profile** If Multistream does not work please make sure that iX application media is allowed in the assigned SIP profile of the endpoint. If not the call will never setup as Multistream. **SX10 Quick Set limitations** SX10 Quick Set does currently not support Multistream in Collaboration Endpoint Software version 8.x. **Hold/Resume (ad-hoc multistream calls)** In CUCM versions < 11.0 SU1 when hold and resume is engaged on a Multistream enabled endpoint, the CUCM will strip away the sip.cisco.multistream header and the TelePresence server will switch to transcoding for this endpoint. This issue is resolved in CUCM 11.0 SU1 and above. **Multistream endpoints only see one PIP from an immersive three-screen system** When a Multistream enabled endpoint, such as SX80, is in call with a three-screen system, such as IX5000, it will not see all

	the three PIP´s from the three-screen system. There will only be one PIP that shows the current Active Speaker. **Bandwidth** Cisco recommends using a minimum default bandwidth of 6 mbps for the full Multistream experience with MX700 and MX800 Dual (two screen systems). Using to low bandwidth may cause the TelePresence Server to fall back to transcoding for the specific endpoint. This is more likely to happen in the event of packet loss. For single screen systems 4 Mbps is recommended. **BugID: CSCuu69550** Mute indication on screen: Participants in a conference that are muted on the server side will not get an indication that they are muted by pressing *6 while in the conference. **BugID: CSCuu69757** Blank site name labels for participants in a Multistream conference: The site name information is missing for meeting deployments that require a conference to be cascaded over more than one TelePresence Server.
Cisco Intelligent Proximity	**Cisco Proximity client for PC (Windows)** "Looking for video systems..." A user might have difficulties pairing to an endpoint running Intelligent Proximity if microphone effects are turned on. Make sure to disable all the microphone effects in the Windows audio settings before attempting to pair to the Proximity endpoint. **Cisco Proximity client for PC (Windows) is currently in beta** The Cisco Proximity application for PC is currently in beta. If you experience any issues with this application we want your feedback. Please post any issues or concerns you may have with the usage of this application on https://www.cisco.com/go/proximity-support. **Intelligent Proximity is only supported with IPv4** The Intelligent Proximity token exchange does not support IPv6 addresses. The mobile device may have an IPv6 address as long as it can connect to the IPv4 addressable endpoint. **One endpoint can have Intelligent Proximity enabled per room** Intelligent Proximity is only supported when just one system per room has this feature enabled. If there are multiple systems with Intelligent Proximity enabled in the same room or in close range, there will be

	interference and device pairing may not work as expected. **OS X El Capitan** If the user has enabled "automatically hide and show the menu bar" under System Preferences -> General, the Cisco Proximity icon will become invisible. **Cisco Proximity version interoperability** Please see the troubleshooting guide for a list of software version constraints.
Touch 10	**Bug ID: CSCum67440** An area may appear dead on the Touch 10 controller's screen if this area has been touched during start-up of the panel. In the start-up phase, a touch calibration process takes place. If something is in contact with the touch panel at this time, this area may lose its function until the Touch 10 has been restarted. Do not touch the touch panel during boot to avoid this.
Active Control	**Bug ID: CSCuo88201** Active Control is set to "Auto" by default. When set to Auto, the endpoint will negotiate it, and if passing over VCS Trunk to CUCM 8.6.2, calls will fail with 503 Service Unavailable. Active Control is supported on CUCM 9.1.2. To work around the issue: Disable Active Control via Conference 1 setting to OFF, or filter it out from VCS side running X8.1.x by changing zone profile to custom and setting SIP UDP/IX filter mode to ON. **BugID: CSCuu28355** When an endpoint dials into a CMR as guest, which should not have permissions to drop any participants, they are still displaying the drop button. When clicked, nothing will happen. This is targeted to be resolved in Collaboration Endpoint Software 8.1.0.
Web interface	**Bug ID: CSCul35568** Due to lack of cipher suite support in IE8 running on Windows XP, HTTPS access is not 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.
SNMP	**Bug ID: CSCtq44757** The Collaboration Endpoint Software is configured with the default SNMP community strings. This is needed for "plug and play" functionality. SNMP community strings should be treated as credentials, and therefore these must be changed after initial configuration.

Security	**Bug ID: CSCtr32420** The codecs shipped with Collaboration Endpoint Software do not meet the Cisco standard passphrase policy. Cisco recommends users to set a passphrase on the system when installed to avoid the system from being compromised.
IPv6	**Bug ID: CSCuo94615** Option 242 from DHCPv6 is not supported on endpoints running Collaboration Endpoint Software.
Management	**Cisco TelePresence Management Server (TMS)** Scheduling conferences using One Button To Push (OBTP) does not work properly using TMS 15.0 and CE8. A fix for this will be implemented in TMS 15.1. **TLS1.0 not supported by endpoints running CE8.1.0 and above.** If the system after upgraded to CE8.1.0 is showing no HTTPS response in TMS, please make sure that TLS1.1 or TLS1.2 is enabled on the TMS server.
Camera Presets	**Bug ID: CSCux71105** When upgrading from TC software to CE software all camera presets are lost. This is a hard limitation and will not be resolved in software.
PresenterTrack	**PresenterTrack is disabled in MultiSite & Multistream calls** The PresenterTrack feature is not available in MultiSite or Multistream calls. **Trigger zone configuration** There is a known limitation when configuring the trigger zone via the web interface; whenever the blue squared is moved around and placed the triggerzone will be saved (regardless if the "save" button is pressed or not. The blue square that is displaying in the selfview on the endpoint do not disappear until the configuration has been saved manually from web or activated the PresenterTrack preset from the Touch 10.
Presentation	**Bug ID: 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.

Interoperability

The interoperability section describes the equipment and software revisions that have been tested for interoperability with this release. Please note: 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
Cisco TelePresence System Video Communication Server (VCS)	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	9.1, 10.0, 10.5, 11.0, 11.5	
Cisco TelePresence System Video Communication Server (VCS)	X8.0, X8.1, X8.2, X8.5. X8.6, X8.7	

Gateway interoperability

Equipment	Software version	Comments
Cisco ISDN Link	IL1.1.5	
Cisco ISDN GW 3241	2.2	

MCU interoperability

Equipment	Software version	Comments
Cisco TelePresence	4.2, 4.3(x.x)	

Server 7010		
Virtual TelePresence Server	4.2, 4.3(x.x)	
Cisco TelePresence Server MSE 8710	4.2, 4.3(x.x)	
Cisco MCU 53xx	4.5(x.x)	
Cisco MCU 42xx	4.5(x.x)	
Cisco MCU 45xx	4.4, 4.5(x.x)	
Cisco CTMS	Not supported	CTMS is not supported with endpoints running Collaboration Endpoint Software.

Streaming servers

Equipment	Software revision	Comments
Cisco TelePresence System Content Server	S5.3, S6.x, TCS7.0, TCS7.1	

Management servers

Equipment	Software revision	Comments
CTS Manager	Not supported	CTS Manager is not supported with endpoints running Collaboration Endpoint Software
TelePresence Management Suite	15.0, 15.1, 15.2	15.2 or later is recommended

Endpoint Interoperability

General information	Known affects endpoints		Comments
H.265 Interoperability	**Polycom** **Lifesize** **Vidyo**		We have observed some interoperability issues with H.265 endpoints (SX80, MX700, MX800 and MX800D) and third-party endpoints. The symptom is no video coming from one or both directions. A workaround that in some cases can rectify the issue is to turn off H.265 on the above Cisco endpoints. From the web interface in "System Configuration" search for "H265" and set the Experimental Conference 1 VideoProtocol DisableH265 to "On".
Cisco	**Software version**	**Protocol**	**Comments**
Cisco TelePresence System 500series 3x00series 1x00series TX9000 TX9200 TX1310	1.10.7 (Ten Bears)	SIP	720p30 max resolution point to point.
Cisco TelePresence System CTS500-32 TX1300 TX9000 TX9200	TX6.0.2 (Lago)	SIP	1080p30/60 support on Lago 1G codecs
Cisco TelePresence MX G1 Series	TC6.x, TC7.x	SIP/H.323	
Cisco TelePresence EX Series	TC6.x, TC7.x	SIP/H.323	
Cisco TelePresence C Series	TC6.x, TC7.x	SIP/H.323	
Cisco IP Video Phone E20	TE4.1.x	SIP/H.323	

Sony	Software version	Protocol	Comments
Sony PCS-1		H.323/SIP	Dual stream is limited to 1 FPS. The main video frame rate will never exceed 15 FPS.
Sony PCS-XG80		H.323/SIP	SIP Far End Camera Control does not work. SIP encrypted calls do not work. SIP/H.323 transfer does not work. Sony is unable to start presentation (BFCP).
Lync	**Software version**	**Protocol**	**Comments**
Microsoft Lync	2013	SIP over VCS trunk from VCS x8	Requires VCS X8 released September 2013.
Polycom	**Software version**	**Protocol**	**Comments**
Polycom VSX 7000		H.323/SIP	At a low video rate and with main video set to sharpness the VSX will not display any video. SIP/H.323 transfer does not work. H.264 is only used on lower bandwidths.
Polycom Real Presence Group 500		H.323/SIP	FECC controls do not work for incoming calls. Unattended H.323 transfer fails on incoming/outgoing calls. No video in unattended SIP transfers from CE to CE for outgoing calls.
Polycom Real Presence Group 300		H.323/SIP	FECC controls not available for outgoing / incoming calls. Unattended H.323 transfer disconnects all calls on outgoing calls. No video in unattended SIP transfers from CE to CE for outgoing calls. Unattended H.323 transfer succeeds but video is lost on both ends on incoming calls.
Polycom HDX 9000		H.323/SIP	
Polycom HDX 8000 HD		H.323/SIP	No video on SIP for outgoing calls to CE endpoints.

Cameras

Equipment	Software revision	Comments
Third party cameras	N/A	Third-party cameras may work with our codecs, but this is not tested and functionality cannot be guaranteed. TAC support may be rejected or limited.

xAPI Changes

The API of Collaboration Endpoint Software has been reduced / changed significantly compared to TC software. We recommend endpoint configuration through the web interface and not from the API command line.

The admin user has access to only a subset of relevant commands and configuration from the API. The admin user can fully manage the system from the web interface where all the configurations are available. The remotesupport user has access to the full list of API commands when utilized (requires TAC engagement).

Specific xAPI changes are not published in the release notes. Please refer to the Cisco API Reference Guides for the integrator products at the following location.

MX series: http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-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

Introduction

Due to occasional updates to hardware components there can be constraints on running older software on newly manufactured endpoints. To identify an 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. 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.

SX10

Compatibility level	Applicable systems	Description	Minimum software version
			CE8
0	SX10	N/A	All
1	SX10	N/A	All
2	SX10	N/A	All
3	SX10	N/A	All

SX80, MX700, MX800 and MX800 Dual

Compatibility level	Applicable systems	Description	Minimum software version
			CE8
0	SX80	N/A	All
0	MX700/MX800/MX800D	N/A	All

SX20, MX200/300 G2

Compatibility level	Applicable systems	Description	Minimum software version		
			CE8		
2	SX20	N/A	All		
3	SX20	N/A	All		
4	SX20	N/A	All		
5	SX20	N/A	All		
0	MX200 G2	N/A	All		
1	MX200 G2	N/A	All		
2	MX200 G2	N/A	All		
0	MX300 G2	N/A	All		
1	MX300 G2	N/A	All		
2	MX300 G2	N/A	All		

Cisco TelePresence Touch 10 hardware dependencies

New hardware revisions for Cisco TelePresence Touch 10

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

The hardware revision number is displayed on the Touch controller during boot in the lower right corner on the touch screen.

Hardware revision	Applicable systems	Description	Minimum software version
			CE8
102300-3 102310-0 102310-1	All	N/A	All supported codec software versions are compatible

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?i=!ch
Cisco TelePresence User Documentation	http://www.cisco.com/go/TelePresence/docs

Software filenames

The correct software filenames are listed in the following table.

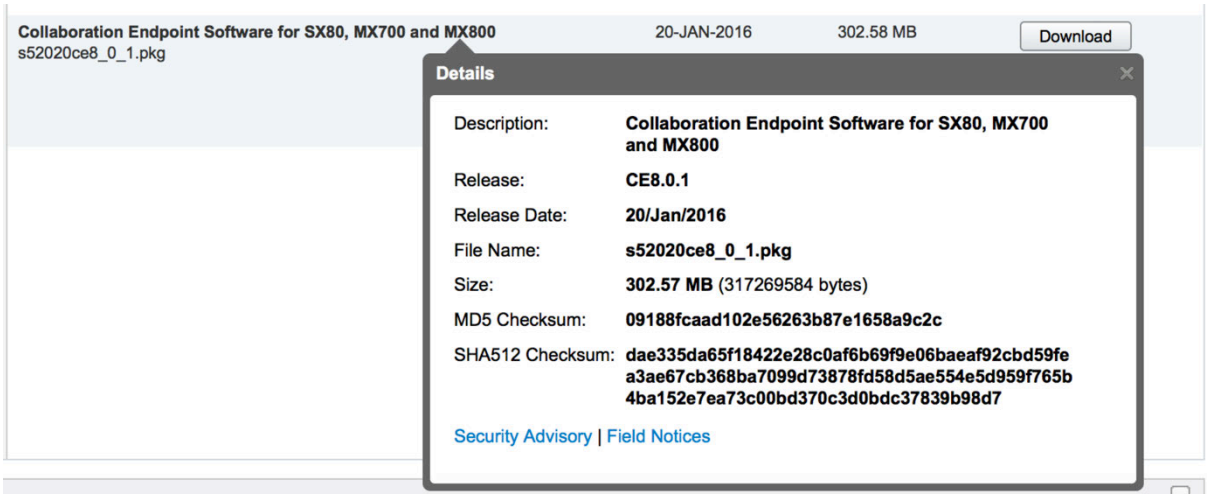
Collaboration Endpoint Software	Software for SX20	Serial range
AES Encryption	s52010ce8_1_1.pkg	All
No Encryption	s52011cenc8_1_1.pkg	All
AES Encryption for CUCM	cmterm-s52010ce8_1_1.k3.cop.sgn	All
No Encryption for CUCM	cmterm-s52011cenc8_1_1.k3.cop.sgn	All

Collaboration Endpoint Software	Software for SX10	Software for MX200 G2, MX300 G2	Software for SX80, MX700, MX800, MX800 Dual	Serial range
Encryption and Non-encryption*	s52030ce8_1_1.pkg	s52010ce8_1_1.pkg	s52020ce8_1_1.pkg	All
Encryption and Non-encryption* for CUCM	cmterm-s52030ce8_1_1.k3.cop.sgn	cmterm-s52010ce8_1_1.k3.cop.sgn	cmterm-s52020ce8_1_1.k3.cop.sgn	All

*SX10, SX80, MX700, MX800, MX800D 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 s52020ce8_0_1.pkg SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 s52020ce8_0_1.pkg

Linux	Open a terminal window and type the following command
	$ sha512sum s52020ce8_0_1.pkg
	Or
	$ shasum -a 512 s52020ce8_0_1.pkg

If the SHA512 checksum matches there is a high level of certainty 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.

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.