Cisco TelePresence

SX, MX, and DX Series

Collaboration Endpoint Software 8

D15314.24

January 2020

Contents

Contents **2**

Document revision history **7**

Introduction to Collaboration Endpoint Software 8 ..... **9**

Important notes and warnings for this software version 9

Equipment and feature considerations before upgrading from TC to Collaboration Endpoint Software 8.x 9

Upgrading from TC to Collaboration Endpoint Software 10

Note well before upgrading from TC to CE 11

Downgrading from Collaboration Endpoint Software to TC 11

CE8.2.1 - New CE to Android conversion load released – (April 2017) 12

CE8.3.1 - New Android to CE conversion load released 12

CE8.3.0 - Advance Notice of Deprecation: MultiStream with Cisco TelePresence Server 13

CE8.3.0 - SHA-1 deprecation 13

Collaboration Endpoint Software on DX - Android to CE conversion load 13

CE8.1.0 - Discontinued support for TLS 1.0 for HTTPS 13

CE8.0.0 - Updated CA certificates for Collaboration Edge 14

Collaboration Endpoint Software cop files for CUCM are signed with RSA3 14

Camera firmware 15

SX20 Quick Set and SX80 camera support 17

Deferred software versions 18

Software and deferral policy 18

CE8.x up to and including CE8.3.7 is deferred 18

CE8.0.0, CE8.0.1, CE8.1.0 deferral for all platforms 18

CE8.0.0 deferral for SX20 18

New features and functionality in CE8.3.8 ..... **20**

New features and functionality in CE8.3.7 ..... **21**

New features and functionality in CE8.3.6 ..... **22**

New features and functionality in CE8.3.5 ..... **23**

New features and functionality in CE8.3.4 ..... **24**

New features and functionality in CE8.3.3 25

New features and functionality in CE8.3.2 26

New features and functionality in CE8.3.1 27

New feature and functionality descriptions CE8.3.1 28

New Startup Wizard behavior for Cisco DX70 and DX80 28

New features and functionality in CE8.3.0 29

New feature and functionality descriptions CE8.3.0 30

New features enabled for Cisco DX70 and DX80 30

Wi-Fi support 30

Intelligent Proximity support 30

In-Room Control 31

UCM feature support 31

IEEE 802.1x authentication is enabled on the Computer Network port 31

In-Room Control: Control external video switcher with virtual sources 32

Active Control support with CMS 2.1 32

Spark on-boarding with LAN paired Touch 10 33

Power save mode on MX700, MX800 and MX800 Dual 33

Minor changes 34

Media channel details visible in xAPI 34

HttpFeedback format options 34

Network speed settings available for Cisco DX70 and DX80, and Cisco TelePresence SX10 34

Advanced setup mode in the initial startup wizard 34

Keypad for DTMF tones available in the web interface under Call Control 34

Intelligent Proximity – Wireless sharing service enabled by default 35

Language support for EnglishUK and SpanishLatin 35

Support for Next Generation Encryption: AES-256 GCM 35

New features and functionality in CE8.2.2 36

New features and functionality in CE8.2.1 37

New features and functionality in CE8.2.0 38

New feature and functionality descriptions CE8.2.0 39

Collaboration Endpoint Software support for Cisco DX70/DX80 39
Cisco Spark on-boarding for the full Collaboration Endpoint Portfolio 41
Touch 10 UI changes 41
H.323 support for Cisco TelePresence SX10 Quick Set 42
Support for LDAP user authentication 42
Touch 10 pairing with non-admin credentials 42
Additional entry points for In-Room Control 43
Minor changes 44
Removal of default option keys 44
New user role: "RoomControl" 44
Multistream requirement update 44

New features and functionality in CE8.1.1 45

New feature and functionality descriptions CE8.1.1 46

CE8.1.1 fixes critical security bug CSCuz26935 (CVE-2016-1387) 46

New features and functionality in CE8.1.0 47

New feature and functionality descriptions CE8.1.0 48

Cisco Spark activation for Cisco TelePresence SX10 Quick Set (CTS-SX10N-K9) 48
New visual design 49
In-Room Control 49
PresenterTrack 50
Intelligent Proximity updates 50
Sharing of mouse pointer 50
Enable and disable Intelligent Proximity services on-screen 50
Direct sharing of presentation to far-end 51
Minor changes 51
On-screen overscan adjustments 51
Support for encrypted active control signaling 51
Audio avatar removed in MultiSite and point-to-point calls 51
Remote logging 51

New features and functionality in CE8.0.1 52

New feature and functionality descriptions CE8.0.1 53

CE8.0.1 fixes a critical bug (CSCux85199) with SX20 Quick Set 53

New features and functionality in CE8.0.0 54

New feature and functionality descriptions CE8.0.0 55

Cisco Intelligent Proximity 55

Content sharing from PC and MAC clients to endpoint via Cisco Proximity 57

Cisco Proximity application availability and requirements 58

Multistream 59

Microphone LED behavior changes 60

Advanced Settings on-screen authentication 61

SX20 Quick Set user interface is aligned with SX10 Quick Set when used with TRC6 61

Supported resolutions 61

1080p presentation resolution on SX10 Quick Set 61

Minor changes 61

DHCP Option 150 is always requested 61

Measure ultrasound-pairing quality using the VU meter 62

Provision endpoints to use HTTPS only from CUCM 62

Snap to Whiteboard improvements 62

Open and resolved caveats in CE8 63

Using the Bug Search Tool 63

Known limitations and advisories 66

Limitations and advisories 66

Interoperability 73

H.323 gatekeepers/traversal servers 73

SIP registrars/proxies 73

Gateway interoperability 73

MCU interoperability 74

Streaming servers 74

Management servers 74

Endpoint Interoperability 75

Cameras 77

xAPI Changes 78

Cisco TelePresence systems hardware dependencies 79

Introduction 79

Cisco TelePresence Touch 10 hardware dependencies.....81

New hardware revisions for Cisco TelePresence Touch 10 81

New hardware revisions for Precision 60 82

Software filenames 83

Software integrity verification 84

Document revision history

Revision	Date	Description
24	January 22nd 2020	Deferral of several software versions due to security issues Minor corrections
23	January 8th 2020	Release of CE8.3.8, minor release with bug fixes
22	April 3rd 2019	Release of CE8.3.7, minor release with bug fixes
21	August 17th 2018	Release of CE8.3.6, minor release with bug fixes
20	June 18th 2018	Release of CE8.3.5, minor release with bug fixes
19	November 24th 2017	Minor corrections
18	November 2nd 2017	Release of CE8.3.4, minor release with bug fixes
17	September 11th 2017	Minor additions to the CE8.3.0 feature section regarding support for AES-256 GCM encryption
16	July 20th 2017	Release of CE8.3.3, minor release with bug fixes. Added info about SNMPv1
15	April 28th 2017	Release of CE8.3.2, minor release with bug fixes New CE to Android conversion release for DX70 and DX80
14	February 1st 2017	Minor corrections
13	January 26th 2017	Release of CE8.3.1, minor release with a new Startup Wizard functionality for Cisco DX Series together with a new Android to CE8.3.1 conversion release for Cisco DX70 and Cisco DX80
12	January 4th 2017	Release of Collaboration Endpoint Software 8.3.0
11	October 19th 2016	New CE to Android conversion release for DX70 and DX80
10	October 4th 2016	Release of CE8.2.2, minor release with bug fixes
09	August 17th 2016	Minor corrections and update regarding Multistream requirements for CE8.2.0
08	July 11th 2016	Update regarding device pack requirements
07	July 8th 2016	Update of release notes as conversion loads for DX70 and DX80 are published on Cisco.com
06	July 1th 2016	Release of CE8.2.1, minor release with bug fixes
05	June 27th 2016	Release of Collaboration Endpoint Software 8.2.0
04	May 4th 2016	Release of CE 8.1.1, minor release with fix for bug CSCuz26935

Revision	Date	Description
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, SX80, Cisco DX80 and DX70 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 are not supported with Collaboration Endpoint Software:

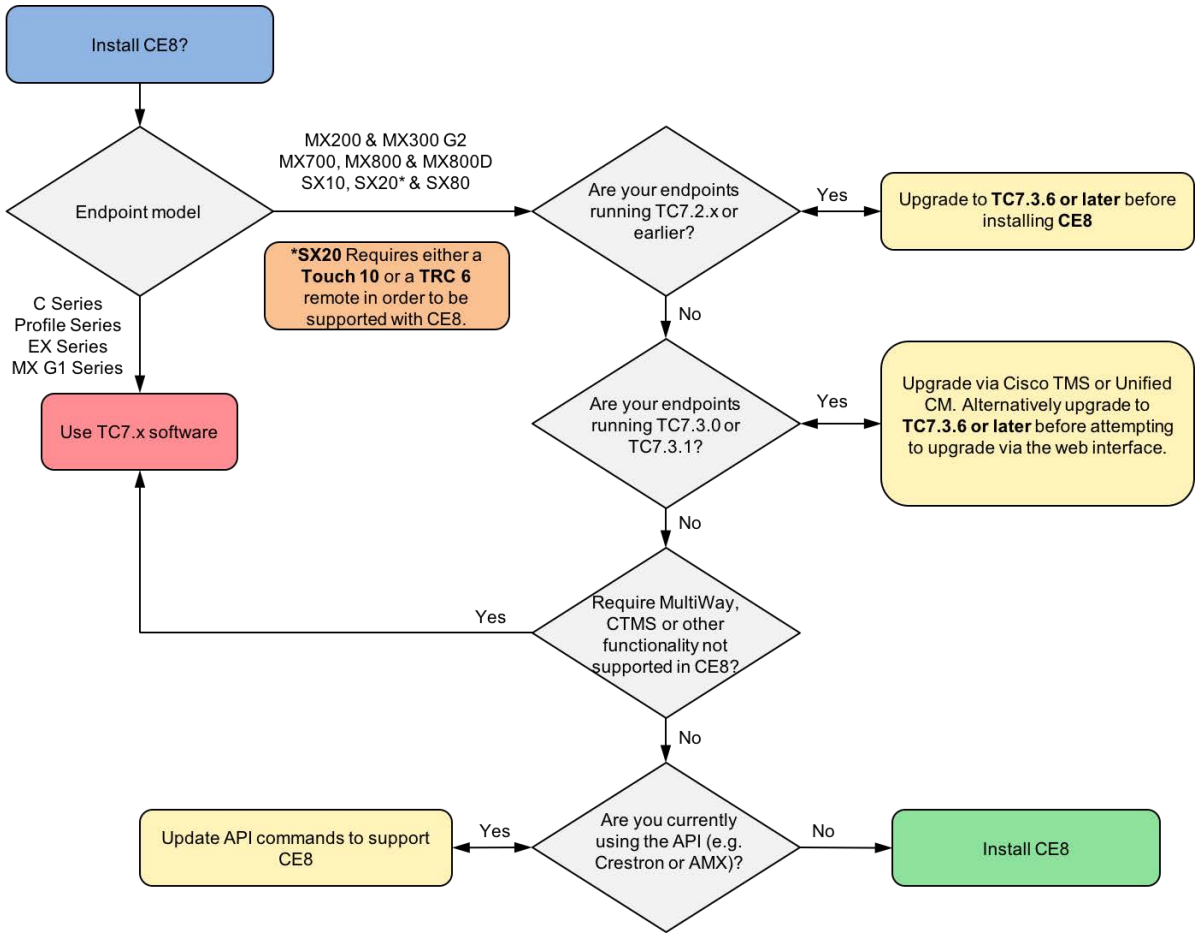
- Cisco TelePresence Touch 8
  - Replaced by the Cisco TelePresence Touch 10
- Cisco TRC5 remote control and below
  - Replaced by the Cisco TRC6 remote for systems that support remote control as a control device i.e. SX20 and SX10
- Multiway
  - Replaced by ad-hoc conferencing (requires CUCM MediaResourceGroupList)
- 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.

Note well before upgrading from TC to CE

- 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.
- Upgrading from TC7.3.3 and later is supported if your endpoint is already running one of these versions. For any other cases, we recommend upgrading endpoints to TC7.3.6 or later before proceeding with the upgrade to Collaboration Endpoint Software. TC7.3.3 through TC 7.3.5 is no longer available for download.
- 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.x to TC7.3.6 or later before downgrading further.

CE8.2.1 - New CE to Android conversion load released – (April 2017)

The previous CE to Android conversion loads is now replaced with new loads.

Old (removed):

- dx80.ce8.2.0-syn213.rel.pkg
- dx70.ce8.2.0-syn213.rel.pkg
- cmterm-dx80-ce820-213-rel-no-default.cop.sgn
- cmterm-dx70-ce820-213-rel-no-default.cop.sgn

New (replacing the Old)

- dx80.ce8.2.0-syn213B.rel.pkg
- dx70.ce8.2.0-syn213B.rel.pkg
- cmterm-ce820-synergy213B.cop.sgn

The new conversion software contains a bug fix for an issue (CSCve12723) that could cause a DX to fail when converting from CE to Android. Note that the fix is applied in the conversion part and not in the Android software. The software version 213B is identical to version 213.

CE8.3.1 - New Android to CE conversion load released

The previous Android to CE conversion loads is now replaced with new loads.

Old (removed):

- cmterm-synergy-ce8_2_1_no_defaults.cop.sgn

New (replacing the Old)

- cmterm-synergy-ce8_3_1_no_defaults.cop.sgn

The difference between the conversion builds is that you now end up in CE8.3.1 that has Wi-Fi support and stability improvements, please read the CE8.3.0 release note below for more information about the included features. Note that you have to downgrade to CE8.2.x if you want to convert back from CE to Android. Please follow the link to the conversion guide for further instructions:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-installation-guides-list.html

Please see the CE9 release notes for newer versions of the conversion software.

CE8.3.0 - Advance Notice of Deprecation: MultiStream with Cisco TelePresence Server

Support for providing a MultiStream meeting experience (i.e. showing participants on both screens on a dual-screen system) is planned for the Cisco Meeting Server (CMS). Focused effort will be allocated on the CMS product and Collaboration Endpoints moving forward. Therefore, support for TelePresence Server based MultiStream implementation is planned for deprecation in a future CE software release.

CE8.3.0 - SHA-1 deprecation

With the planned deprecation of SHA-1 by the most popular browsers early 2017, all self-signed certificates on endpoints running CE8.3.0 are regenerated with SHA-2 signature. If you have problems connecting to the web interface of the codec, please make sure your browser supports SHA-2.

Collaboration Endpoint Software on DX - Android to CE conversion load

The Android to Collaboration Endpoint Software conversion load is depending on the following CUCM device packages.

- CUCM 11.5.1: cmterm-devicepack11.5.1.11001-2.cop.sgn
- CUCM 11.0.1: cmterm-devicepack11.0.1.22049-2.cop.sgn
- CUCM 10.5.2: cmterm-devicepack10.5.2.14076-1.cop.sgn
- CUCM 9.1.2: cmterm-devicepack9.1.2.16137-1.cop.sgn

The conversion loads are now available on Cisco.com. Ensure the relevant device packs are installed on Cisco UCM before the conversion from Android to CE. Please refer to the conversion guide located here: https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce82/dx80-dx70-convert-between-CE-android-based-software.pdf

CE8.1.0 - Discontinued support for TLS 1.0 for HTTPS

Cisco TelePresence Endpoints running CE8.1.0 and above 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 or above. 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.x.

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.

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.x 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
CE8.3.8	Precision 60 55000000	HC8.3.8.0b92a8a	
CE8.3.7	Precision 60 55000000	HC8.3.7.470b0a5	
CE8.3.6	Precision 60 55000000	HC8.3.6.5045787	
CE8.3.5	Precision 60 55000000	HC8.3.5.c877c7f	
CE8.3.4	Precision 60 55000000	HC8.3.4.99243f7	
	PrecisionHD 1080p 4x S2 / Precision 40 53000000	S01777-2.2 RC17 ID: 20040	
CE8.3.3	Precision 60 55000000	HC8.3.3.7064ff0	
	PrecisionHD 1080p 4x S2 / Precision 40 53000000	S01777-2.2 RC15 ID: 20038	
CE8.3.2	Precision 60 55000000	HC8.3.2.a715ecb	
CE8.3.1	Precision 60 55000000	HC8.3.1.3276302	
CE8.3.0	Precision 60 55000000	HC8.3.0.c1a7707	
	PrecisionHD 1080p 12x / Precision 12x 5000000(1-5)	S01718-4.0 FINAL ID:40085	
CE8.2.2	Precision 60	HC8.2.2.3263c59	

	55000000		
CE8.2.1	Precision 60 55000000	HC8.2.1.e9daf06	
CE8.2.0	Precision 60 55000000	HC8.2.0.d66bc59	
	PrecisionHD 1080p 2.5x 54000000	S01777-2.2 RC14 ID:20037	
	PrecisionHD 1080p 4x S2 / Precision 40 53000000	S01777-2.2 RC14 ID:20037	
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 / Precision 40 53000000	S01777-2.2 RC12 ID:20035	
	PrecisionHD 1080p 12x / Precision 12x 5000000(1-5)	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 Precision 40	Full support
	PrecisionHD 1080p 12x	Full support
SX80	Precision 60	Full support
	SpeakerTrack 60	Full support
	PrecisionHD 1080p 4x S2 Precision 40	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 and installing affected software versions. Replacement software will always be in place before a software version is deferred.

Software and deferral policy

Older software versions will be deferred on a regular basis from the download section on cisco.com to avoid providing potential vulnerable software after security fixes. As a general rule you will from January 2020 be able to download the latest release and the version before. Older software versions will be removed from cisco.com.

Example:

If CE8.3.8 and CE8.3.9 is released and CE8.3.10 becomes available, CE8.3.8 will be removed.

X.X.x = major . minor . maintenance

CE8 software is in maintenance mode and security fixes is applies until end of maintenance. This means that there will not be any new minor release for CE8, only maintenance releases for CE8.3.x.

CE8.x up to and including CE8.3.7 are deferred

All CE8.x versions up to and including CE8.3.7 are deferred due to a discovered vulnerability in the affected software versions. Please refer to the deferral notice for more information.

https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/ce9/release-notes/TC7-CE8-CE9-deferral-notice.pdf

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 CE8.3.8

- Minor release and contains only bug fixes.
  - Please see the “Open and resolved caveats” section in this document.
  - Resolved security issues related to CVE-2020-3143
    - CSCvs67680
    - CSCvs45241

    For more information please read the official Security Advisory
    - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-telepresence-path-tr-wdrnYEZZ

    Earlier affected software versions have been removed and is no longer available to download, please read the software deferral notice for further details.
    - https://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/ce9/release-notes/TC7-CE8-CE9-deferral-notice.pdf

New features and functionality in CE8.3.7

- Minor release and contains only bug fixes.
    - Please see the “Open and resolved caveats” section in this document.

New features and functionality in CE8.3.6

- Minor release and contains only bug fixes
    - Please see the “Open and resolved caveats” section in this document.

New features and functionality in CE8.3.5

- Minor release and contains only bug fixes
    - Please see the “Open and resolved caveats” section in this document.

New features and functionality in CE8.3.4

- Minor release and contains only bug fixes
    - Please see the “Open and resolved caveats” section in this document.
- Fixes WPA2 related vulnerabilities (KRACK) – CSCvf71761

New features and functionality in CE8.3.3

- Minor release and contains only bug fixes
    - Please see the “Open and resolved caveats” section in this document.
- Applied a filter to increase speech intelligibility on G.729 codec.

New features and functionality in CE8.3.2

- Minor release and contains only bug fixes
    - Please see the “Open and resolved caveats” section in this document.
- A new CE to Android conversion build for Cisco DX70 and Cisco DX80 has been released. You can find the new conversion build under the CE8.2.1 version on cisco.com. Conversion from CE to Android is only supported in CE8.2.x.

New features and functionality in CE8.3.1

- Minor release
- New Startup Wizard behavior on Cisco DX70 and DX80
- A new Android to CE conversion build for Cisco DX70 and Cisco DX80 has been released together with CE8.3.1

New feature and functionality descriptions CE8.3.1

New Startup Wizard behavior for Cisco DX70 and DX80

If the initial Startup Wizard is displayed on the Cisco DX70 and DX80, it will attempt to register to UCM via DHCP option 150 after a timeout period of 8 minutes.

- After 4 minutes a notification will be displayed on-screen that the system will be automatically provisioned (if option 150 is detected).
- If option 150 does not exist, the system will not do anything and wait until you have completed the Startup Wizard manually.
- If provisioning fails after the initial 8-minute timeout, the system will retry registration every 2 minutes. After a registration attempt the wizard will be turned off, so any further configuration should be performed from the web interface if required.
- If you start going through the Startup Wizard, the countdown will be cancelled and you have to complete the wizard manually.

This behavior is implemented to reduce the need for user interaction if option 150 is used for UCM provisioning. By using the new Android to CE8.3.1 conversion build this functionality is enabled automatically after a successful conversion.

New features and functionality in CE8.3.0

- New features enabled for Cisco DX70 and DX80
    - Wi-Fi support
    - Intelligent Proximity support
    - In-Room Control
    - UCM feature support
        - Voicemail, forward all calls, shared lines, consultative add and transfer, extension mobility, multiple calls on hold and merge calls
    - IEEE 802.1x authentication enabled on the Computer Network port
- In-Room Control: Control external video switcher with virtual sources
- Active Control support with CMS 2.1
- Spark on-boarding with LAN paired Touch 10
- Power save mode on MX700 and MX800 series
- Minor changes
    - Media channel details available in xAPI
    - HttpFeedback format options
    - Network speed settings added for Cisco DX70/DX80 and SX10
    - Advanced setup mode in the initial startup wizard
    - Keypad for DTMF tones available from the web interface under Call Control
    - Wireless sharing from laptop via Proximity enabled by default for all systems
    - Language support for EnglishUK and SpanishLatin
    - Support for Next Generation Encryption: AES-256 GCM

New feature and functionality descriptions CE8.3.0

New features enabled for Cisco DX70 and DX80

Wi-Fi support

Wi-Fi support has been enabled in CE8.3.0 for Cisco DX70 and DX80 systems that are shipped with a built-in Wi-Fi adapter.

Supported IEEE standards	Supported security protocols
IEEE802.11n, IEEE802.11a, IEEE802.11g, IEEE802.11b	WPA-PSK (AES), WPA2-PSK (AES)

Support for additional enterprise security protocols will come in a later Collaboration Endpoint Software release.

Access the network settings in the on-screen user interface to connect to a wireless network. In order to use Wi-Fi, you must disconnect the Ethernet cable if connected. A notification will be displayed if the system detects that you are connected with an Ethernet cable and that you cannot proceed until you have disconnected the Ethernet cable.

Ethernet will always take precedence over Wi-Fi if connected.

If the network you are trying to connect to is not supported it will be displayed on-screen, the DX system does not support the security protocol for that network.

Intelligent Proximity support

Intelligent Proximity is now supported on the Cisco DX70 and DX80 in alignment with other endpoints running Collaboration Endpoint software. The feature is disabled by default and must be enabled in the configuration. Cisco only supports one endpoint per room that has Proximity enabled. Multiple systems transmitting ultrasound in close proximity of one another causes noise and unstable pairing conditions.

All the Proximity services, wireless sharing, receive content and endpoint control via the Proximity clients are supported with the DX systems. Please note that paired devices will only be able to receive content when shared to the far-end in a call, if the content is “previewed” it will not be sent to the paired devices regardless if the content is previewed inside or outside of a call due to privacy concerns.

Only three simultaneous Proximity connections are supported with the DX70 and DX80 at a time.

In-Room Control

In-Room Control can be enabled on the Cisco DX70 and DX80 to control lights, blinds or other peripherals in the room.

Please read the In-Room Control guide available here for more information on how to use this feature:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/products-installation-and-configuration-guides-list.html

Not that there is a limitation relating to the graphical rendering of widgets. See the known limitation and advisories section for more details.

UCM feature support

CE8.3.0 enables multiple UCM features on the Cisco DX70 and DX80 that is also supported on the other endpoints in the Collaboration Endpoint portfolio.

- Voicemail
- Shared lines
- Extension Mobility
- Forward all calls
- Consultative add and transfer
    - Consultative add/transfer allow you to consult with the participant you intend to add or transfer and send DTMF tones before completing the add/transfer.
- Multiple calls on hold and merge calls (using MGRL)

IEEE 802.1x authentication is enabled on the Computer Network port

Enables IEEE 802.1x authentication on the Computer Network port on the Cisco DX70 and DX80. Devices connected to this port can authenticate using IEEE 802.1x authentication.

In-Room Control: Control external video switcher with virtual sources

This feature allows you to extend the physical input source(s) on a Cisco TelePresence video system (including Cisco DX70 and DX80) into virtual sources that represents each input source on one or more video switchers. The virtual sources are visible from the share tray (on-screen or on the Touch 10) and can be presented as any other physical source without needing to swap cables or change input source manually. It will look completely transparent for normal users.

The number of virtual sources you can create depends on how many you have available on the video switcher; Cisco recommends no more than maximum 50 virtual sources.

The external video switcher must be supported by a control system, for example from Crestron or AMX, that can interact with the video systems API to make this feature work.

For more information on how to setup virtual sources, please follow the link below:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/products-installation-and-configuration-guides-list.html

Active Control support with CMS 2.1

Active Control is a SIP feature that has been supported with Cisco TelePresence endpoints for a while with Cisco TelePresence Server. The Active Control feature allows the conference participants to receive details of the meeting and perform a few administrative tasks during the meeting, using the endpoint user interface. This includes a participant list (roster list) showing who is speaking, sharing, muted. You can actively drop participants, mute, change layout etc.

This feature is now supported on CMS 2.1 hosted conferences and endpoints running CE8.3.0.

Active Control is default set to “Auto” on the Room Systems and will be negotiated automatically if available on the CMS side.

A few highlights that was previously not available is that Active Control will tell the endpoint when it is muted on the server side and the mute indicator will glow red on the endpoint. You can unmute yourself by pressing the mute button on the microphone, remote control or Touch 10 just like any normal scenario instead of sending DTMF signals to the conference server.

- Best effort encryption by default.
- Adaptive layouts based on active speakers.
- Recording status indicator.
- Active Control features are also available from the call control area of the web interface.

Spark on-boarding with LAN paired Touch 10

It is no longer required that the Touch 10 is directly paired to the video endpoint to offer Spark as an activation alternative. While the system is in factory reset state and displaying the “Welcome” screen, pair the Touch 10 to the system IP address and follow the steps on the Touch 10.

This also enables Touch 10 operation for systems previously only supported with the TRC 6 remote control while activated on Spark, such as the Cisco TelePresence SX10 and SX20.

The Spark Room System must be running CE8.3.0 from a factory default state in order to on-board to Spark with a LAN paired Touch 10. The “Welcome” screen must be visible and the wizard must not be completed. Pair the Touch 10 to the Room System while in this state and follow the steps on the Touch 10.

Updated requirements for Spark registration for the below Room Systems (factory default state, CE8.3.0):

Spark Room System	CE Version	Touch 10 (Direct)	Touch 10 (LAN)	TRC6
SX10, SX10N	CE8.3.0	No	Yes	Yes
SX20, SX20N	CE8.3.0	No	Yes	Yes
SX80	CE8.3.0	Yes	Yes	No
MX200 G2/MX300 G2	CE8.3.0	Yes	Yes	No
MX700/MX800/MX800D	CE8.3.0	Yes	Yes	No
DX70/DX80	CE8.3.0	N/A (use touch screen)	N/A (use touch screen)	N/A

Power save mode on MX700, MX800 and MX800 Dual

“Power save” mode is designed to reduce power consumption while the system is not in use over time, for example during out of office hours and weekends. The feature is an extension of the normal standby mode but is disabled by default. To enable “power save” mode we recommend to configure a power save schedule (out of office hours) from the web interface of the video system.

When the system enters “power save” mode, power supply to the integrated cameras are turned off and will save approximately 15 watts per camera while in “power save” mode. The video system will automatically wake up from power save mode 5 minutes before it enters the normal office hours and use regular standby mode for the configured duration. The power save schedule is available from the “Time” configuration and activated by setting “PowerSave” to “OutsideOfficeHours” within the “Standby” configuration.

The codec can make and receive calls instantly when waking up the system but since the cameras must boot it takes approximately 1:45 minutes before you will see the self-view and the system starts sending video to the far-end. Note that this is only valid if you wake the system during out of office hours and Power Save mode is enabled.

Minor changes

This section covers a set of relevant minor changes introduced in Collaboration Endpoint Software 8.3.0.

Media channel details visible in xAPI

Media channel information on packet loss and jitter while in a call is now visible in the xAPI. To see the media channel details, you can run xStatus MediaChannels from the xAPI as the admin user while in a call.

HttpFeedback format options

HttpFeedback format can be set to JSON (JavaScript Object Notation) as an alternative to XML (eXtensible Markup Language) for third party interpreters or REST API´s. TMS will provision the HttpFeedback as XML by default automatically and will never use JSON as it does not support it.

Network speed settings available for Cisco DX70 and DX80, and Cisco TelePresence SX10

Configurable from the web interface or in the xAPI.

Advanced setup mode in the initial startup wizard

If you do want to manually setup the system or use a third party application, you can select the “Advanced Setup” mode in the provisioning wizard.

Keypad for DTMF tones available in the web interface under Call Control

When dialing from the web interface, a keypad is available to send DTMF tones to the far end if required.

Intelligent Proximity – Wireless sharing service enabled by default

Wireless sharing is a service provided by Intelligent Proximity. Wireless sharing, which allows a laptop to share content to a video system, is now enabled by default. Please note that Intelligent Proximity mode must be enabled in order to pair a laptop to a video system through the Cisco Proximity desktop client. Pairing is required before you can use the wireless sharing service.

Intelligent Proximity mode is only enabled by default on the integrated systems like Cisco TelePresence MX200 G2, MX300 G2, MX700, MX800 and MX800D with the exception of DX70 and DX80.

Language support for EnglishUK and SpanishLatin

We have added support for EnglishUK and SpanishLatin to the on-screen display and user interfaces.

Support for Next Generation Encryption: AES-256 GCM

Added support for AES-256 GCM encryption algorithm for SIP.

New features and functionality in CE8.2.2

- This is a minor release and contains only bug fixes, including security fixes.
- Some changes with the “add” button logic in relation to a resolved bug in this release.
    - Please see the known limitations under the CUCMMediaResourceGroupList section in this document for more information.

New features and functionality in CE8.2.1

- This is a minor release and contains only bug fixes

New features and functionality in CE8.2.0

- Collaboration Endpoint Software support for Cisco DX70 and DX80
- Cisco Spark on-boarding for the Collaboration Endpoint portfolio
- Touch 10 UI changes
- H323 support for Cisco TelePresence SX10 Quick Set
- Support for LDAP user authentication
- Touch 10 pairing with non-admin credentials
- Additional entry points for In-Room control
- Minor changes
- Removal of default option keys
- New user role: "RoomControl"
- Added language support for Canadian French - Français (Canada)
- Multistream requirement updates

New feature and functionality descriptions CE8.2.0

Collaboration Endpoint Software support for Cisco DX70/DX80

Cisco DX70 and Cisco DX80 with software version 10.2.5.212 and above can be converted to Collaboration Endpoint Software.

This process removes the Android-based operative system and all apps, and the system becomes a pure TelePresence device aligned with the Collaboration Endpoint portfolio, and most of its features. The Cisco DX70 and DX80 can, after the conversion, be upgraded further using the normal process and packages. Reverting from Collaboration Endpoint Software is supported only from CE8.2.x.

For instructions on how to convert a Cisco DX70 or DX80 to Collaboration Endpoint Software, or to revert back to the Android-based OS, see the conversion guide:

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce82/dx80-dx70-convert-between-CE-android-based-software.pdf

See the administrator guide for instructions on how to operate the system after the conversion to Collaboration Endpoint Software:

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce82/dx70-dx80-administrator-guide-ce82.pdf

Note: Converting from the Android-based OS to Collaboration Endpoint Software requires UCM. If you do not have a UCM in your environment to perform the conversion, please open a case with Cisco Technical Assistance Center.

Note: Cisco DX650 is not supported for conversion to Collaboration Endpoint Software, only Cisco DX70 and DX80.

Note: CUCM 9.1.2, 10.5.2, 11.0.1 and 11.5.1 requires a new device pack in order for the CUCM to recognize the new device after the conversion process:

CUCM 11.5.1: No device pack currently available

CUCM 11.0.1: cmterm-devicepack11.0.1.22048-1.cop.sgn

CUCM 10.5.2: cmterm-devicepack10.5.2.14076-1.cop.sgn

CUCM 9.1.2: cmterm-devicepack9.1.2.16137-1.cop.sgn

It is important to note before you convert your DX Series endpoint that Collaboration Endpoint Software is different from the Android-based OS. Many features available in the Android-based OS are not available after converting to CE. On the other hand, many features not available in the Android-based OS are available in CE.

Features supported in CE8.2.0 on DX Series*		**DX Specific in CE8.2.0**
Spark / UCM / VCS Registration	HDMI-in audio	Full touch operated screen
LED missed call indicator	Hold/Resume	Jabra 450 for Cisco handset
TMS provisioning and directories	DTMF	Plantronics P240 wired handset
ClearPath resilience	Add favorites	USB headsets**
H263/H264	“Camera closed” indicators	
SIP/H323	One Button to Push (OBTP)	* Only the most relevant features are mentioned in this list. More features and functionalities will be added in future CE releases
Document camera	Content sharing (1080p5)	**A list of known working and tested USB headsets can be found here:
FECC – Far End Camera Control	Do not disturb	http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/ce82/dx70-dx80-user-guide-ce82.pdf
PC monitor (1080p60)	Full web access	
Expressway	Remote monitoring option PID: L-DX-SERIES-RM	

Features not supported in CE8.2.0, but may be included in a future release	
Wi-Fi (Released in CE8.3.0)	Edit favorites (Released in CE8.3.0)
Bluetooth	Extension mobility (Released in CE8.3.0)
Transfer call (Released in CE8.3.0)	OSD mute indicator (Mute LED glows red when muted)
Forward all (Released in CE8.3.0)	Audio cone (Released in CE8.3.0)
Shared lines (Released in CE8.3.0)	Non-QWERTY keyboard language localization
Concierge	Keyboard control
Voicemail (Released in CE8.3.0)	Keyboard and mouse re-direction
Auto answer (Released in CE8.3.0)	In-Room control (Released in CE8.3.0)
Ringtone and wallpaper options in the UI	
Intelligent Proximity (Released in CE8.3.0)	

For more information, please refer to the DX Administrator Guide

Cisco Spark on-boarding for the full Collaboration Endpoint Portfolio

Cisco Spark on-boarding is from CE8.2.0 supported for the full Cisco TelePresence Collaboration Endpoint portfolio, which includes the Cisco TelePresence SX10 (SX10N from CE8.1.0), SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, MX800 Dual, DX70, and DX80.

Cisco TelePresence SX10, SX10N, and SX20 only support on-boarding to Cisco Spark, if operated with a TRC6 infrared remote control.

SX80, MX200 G2, MX300 G2, MX700, MX800, and MX800D require a directly paired Touch 10 panel. If the Touch 10 is not directly paired to the codec, you will not see the option to register the system to Cisco Spark.

For more information about Cisco Spark and how to get your endpoints activated on Cisco Spark, please visit https://www.ciscospark.com/

Basic requirements for Spark registration for the below Room Systems (factory default state):

Spark Room System	Min. CE Version	Touch 10	TRC6	Encryption Option Key
SX10N (CTS-SX10N-K9)	CE8.1.0	No	Yes	Yes 8.1.0 (No CE8.2.0)
SX10 (CTS-SX10-K9)	CE8.2.0	No	Yes	No
SX20	CE8.2.0	No	Yes	No
SX80	CE8.2.0	Yes	No	No
MX200 G2/MX300 G2	CE8.2.0	Yes	No	No
MX700/MX800/MX800D	CE8.2.0	Yes	No	No
DX70/DX80	CE8.2.0	N/A	N/A	N/A

Touch 10 UI changes

A visual update has been applied to the Setup and Pairing Wizard on the Touch 10. The Touch 10 has a new GUI when registered to Cisco Spark, which is similar to the Cisco TelePresence SX10 on-screen user interface. If the endpoint is registered to on-premise infrastructure, the Touch 10 panel boots into the user interface known from, for example CE8.1.1.

H.323 support for Cisco TelePresence SX10 Quick Set

The Cisco TelePresence SX10 Quick Set has added support for the H.323 protocol in alignment with other endpoints in the Collaboration Endpoint portfolio.

Support for LDAP user authentication

A new configuration set has been added to support admin user authentication towards an LDAP service for all Collaboration Endpoints that are running CE8.2.0 and above. Please note that the local admin user will always be present and active.

The LDAP feature works with any standard LDAP service, for example Microsoft Active Directory. It is enabled and configured through the web interface/API of the codec, or bulk provisioned by UCM.

See instructions below on how to log in with LDAP credentials after the endpoint is correctly configured to use an LDAP service for authentication:

- Web: <domain>\<LDAP username> or <LDAP username>@<domain>
- Touch 10 Administrator settings: <LDAP username>@<domain>
- Secure shell: ssh -l <LDAP username>@<domain> <codec-IP>
    - Note that logging in via SSH and Touch 10 does not support the <domain>\<LDAP username> format
    - Touch 10 cannot be paired to the endpoint using LDAP credentials

The endpoint connects to the LDAP service directly to authenticate the user. All the users that can authenticate through the LDAP service will be administrators; this feature does not support non-admin user roles.

Touch 10 pairing with non-admin credentials

The Touch 10 panel can be paired remotely to a codec running CE8.2.0 and above using non-admin or admin credentials. Only the "User" role is required.

When the Touch 10 is successfully paired, admin credentials are required to modify the Administrator settings as before for example, un-pairing the Touch 10 panel from the codec.

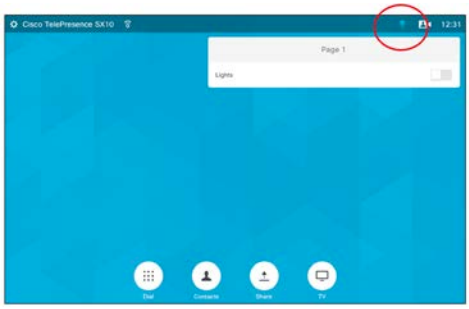
This feature may simplify scenarios where non-admin users on-site are in a situation where they must pair the Touch 10 to the codec for any reason. An administrator can create a regular user intended for this scenario, and provide these credentials to the user without compromising security. The regular user can safely be deleted from the codec after the Touch 10 panel has been paired successfully.

Additional entry points for In-Room Control

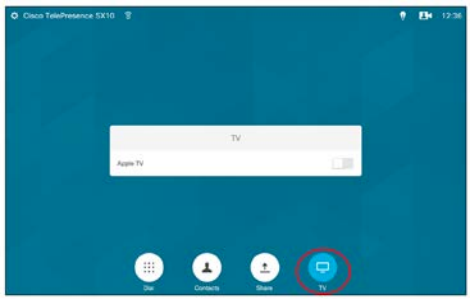
In-Room controls now provides two additional entry points that allow you to create contextual room control. There are three entry points in total; Global, Homescreen and In-Call. In addition, a wider selection of entry point icons has been included in the In-Room control editor.

Global	**Homescreen**	**In-Call**
Recommended features: ▪ Lights ▪ Blinds ▪ Ventilation Available in and out of call	Recommended features: ▪ TV ▪ Services ▪ Media Available outside of call only	Recommended features: ▪ Microphones ▪ Recording ▪ Help Available inside of call only

- Global



- Homescreen



- In-Call

Minor changes

This section covers a set of relevant minor changes introduced in Collaboration Endpoint Software 8.2.0.

Removal of default option keys

The following options keys are included by default on most Collaboration Endpoints, and are no longer listed as an option key from CE8.2.0:

- NaturalPresenter
- DualDisplay
- HighDefinition
- PremiumResolution

The functionality these option keys provided is still available, but the keys have become redundant.

Any pre-installed keys are stored on the codec, in case you have to downgrade to software versions that require these option keys to enable the respective functionalities after the downgrade.

New user role: "RoomControl"

The "RoomControl" user role is added to provide non-admin users or integrators access to the In-Room control editor. The "RoomControl" role can be assigned when a new non-admin user is created from the codec's web interface.

Multistream requirement update

Multistream requires Cisco UCM 11.0.1 with this release, please see the known limitations section under Multistream for more information.

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
- Remote logging

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:

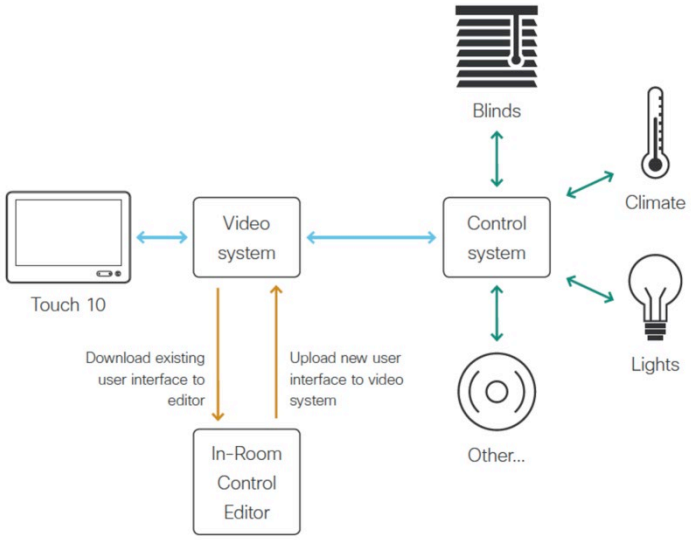
https://help.webex.com

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 setup 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.

Remote logging

Remote logging of the full codec logs using Syslog or SyslogTLS is now supported. In previous versions the remote logging feature would only log audit events for security concerns to a Syslog server. The feature is configured in the codec web interface under Setup -> Configuration -> Logging.

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
- “Add” button behavioral changes

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.

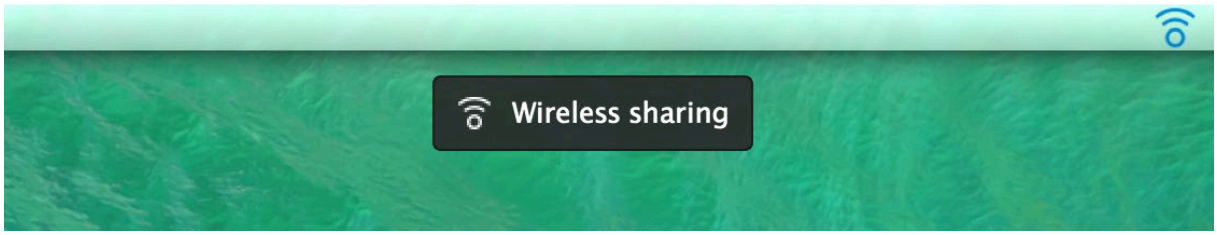
The integrator systems (SX series) have Cisco Intelligent Proximity pairing mode disabled by default, because we cannot account for how these devices are being setup together with third party equipment. Intelligent Proximity pairing mode must be enabled manually for the SX series.

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 supported from client version 2.0.0. Previous versions was 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

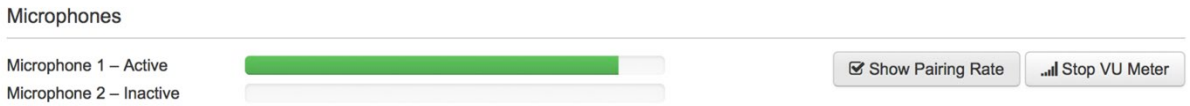
This section will cover a set of relevant minor changes introduced in Collaboration Endpoint Software 8.0.0.

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
CE8.3.8	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.8&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8&sb=anfr&sts=open&bt=custV
CE8.3.7	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.7&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.7&sb=anfr&sts=open&bt=custV
CE8.3.6	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.6&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.6&sb=anfr&sts=open&bt=custV
CE8.3.5	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.5&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.5&sb=anfr&sts=open&bt=custV

CE8.3.4	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.4&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.4&sb=anfr&sts=open&bt=custV
CE8.3.3	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.3&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.3&sb=anfr&sts=open&bt=custV
CE8.3.2	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.2&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.2&sb=anfr&sts=open&bt=custV
CE8.3.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.1&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.1&sb=anfr&sts=open&bt=custV
CE8.3.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.0&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.3.0&sb=anfr&sts=open&bt=custV
CE8.2.2	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.2&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.2&sb=anfr&sts=open&bt=custV
CE8.2.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.1&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.1&sb=anfr&sts=open&bt=custV
CE8.2.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.0&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.2.0&sb=anfr&sts=open&bt=custV
CE8.1.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.1&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.1&sb=anfr&sts=open&bt=custV

CE8.1.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.0&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.1.0&sb=anfr&sts=open&bt=custV
CE8.0.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.1&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.1&sb=anfr&sts=open&bt=custV
CE8.0.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.0&sb=fr&sts=fd&bt=custV	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283661039&rls=8.0.0&sb=anfr&sts=open&bt=custV

Known limitations and advisories

Limitations and advisories

Equipment / Feature	Summary
Spark activation	Spark activation can only be performed from the startup wizard and requires the system to be in factory reset state. From CE8.3.0 spark activation can be performed from a LAN paired Touch 10. The Touch 10 must be paired to the video system on LAN while the Startup Wizard is active before the system is activated. There are no options to pair/re-pair a Touch 10 once activated on Spark.
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. Please note that being registered to CUCM without having provisioning mode set to “CUCM” is not a supported scenario. **NTP** The collaboration endpoints do not support broadcast NTP servers from CUCM, unicast only.
CUCMMediaResourceGroupList	**Adding participants with MRGL** Valid from CE8.0.0 through CE8.2.1: If you are already connected to an MCU it is not possible to add/merge an incoming call. The “Add” button is replaced with “Answer & Hold” in the incoming call dialog. When you dial into an MCU hosted conference the opportunity to add additional participants was removed to avoid cascaded conferences as this may break content share functionality between the cascaded conferences. From CE8.2.2: The above change has been modified and the “add” button is available. Keep in mind that if you “add” a participant while already in an MCU call, a cascaded conference may be created (connecting two conferences on two different MCUs hosted at different locations) and content sharing between the two conferences may not work as

	expected in this scenario.
Cisco TelePresence 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-CODEC 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*
Cisco TelePresence SX10 Quick Set	**H.323** H.323 is not supported on this endpoint running software < CE8.2.0. *Added support for H.323 from CE8.2.0* **Audio issues (CSCvb27626 and CSCvb87521)** When downgrading from CE8.x to TC software two different audio issues can occur that causes audio on HDMI output and/or HDMI input is lost. To resolve both issues, please factory reset the system.
Cisco TelePresence 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.
Cisco DX70 & DX80	**Please see the "New feature and functionality descriptions" section for a list of un-supported features in CE8.2.0.** **In-Room Control (CE8.3.0)** There is a limitation that is causing a low resolution of widgets to appear large and pixelated. This is planned to be resolved in a later release of CE software.
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. *Resolved in CE8.3.0*
SIP	**SIP Listen Port** We recommend that SIP Listen Port is turned off when registered to a SIP proxy for example, VCS.

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 when using CE8.
Multistream	**CE8.2.0 requires CUCM 11.0.1 for Multistream** In order to continue using Multistream with CE8.2.0, CUCM 11.0.1 is required. Due to several bug fixes with CUCM 11.0.1 and Multistream this requirement was introduced with CE8.2.0. **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. *Resolved in CE8.2.0* **Multistream SIP SDP message size can be too large for CUCM** The symptom is that the call is failing. CUCM version < 11.0.1 has a default SIP Max incoming message size of 11000 bytes (also includes upgrades to CUCM 11.0.1). 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. CUCM 11.0.1 and above is required 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. **Cisco DX70, DX80 and Cisco TelePresence SX10 Quick Set** These video systems do not support Multistream. **Hold/Resume (ad-hoc multistream calls)** In CUCM versions < 11.0.1 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 11.0.1 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.
Cisco Intelligent Proximity	**Please refer to the Cisco Support Forums for questions and support** http://www.cisco.com/web/go/proximity-support **Troubleshooting guide** https://supportforums.cisco.com/document/12159326/troubleshooting-guide-cisco-proximity **Strong Security mode (JITC)** If strong security mode is enabled, Proximity traffic will intentionally be blocked by the Collaboration Endpoint. Proximity should be turned off while the system has Strong Security mode enabled.
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. **After upgrading from TC to CE the Touch 10 may need to be rebooted** A limitation with the software may cause a remotely paired Touch 10 to hang after an upgrade from TC to CE. In order to resolve this issue, unplug the Touch 10 and re-plug it so the Touch 10 will reboot.

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. *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. **Bug ID: CSCvf26748** SNMPv1 is removed in CE 8.3.2 and onwards. Cisco recommends utilizing supported versions of SNMP.
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.
Encryption	**Bug ID: CSCvd33159** The AES-256 encryption algorithm (supported for SIP from CE8.3.0) may cause some interoperability issues with endpoints that do not have support for this, for example E20. From CE8.3.3 and CE9.1.3 this algorithm can be filtered away by adding it to the codec cap set filter to work around these issues.
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. **TLS 1.0 for HTTPS 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.
Startup Wizard	While the Startup Wizard is active and displayed on screen or on the Touch 10, the system will have “Do Not Disturb” mode enabled by design. The DND mode cannot be turned off while the Startup Wizard is active. To remove the Startup Wizard, finish the Startup Wizard normally by following the steps or turn off the “RunStartupWizard” by setting the value to “False”. This must be done from the web interface and to find the setting you must search for it in the configuration search field.
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.

H.323	From CE8.3.0 the default value of xConfiguration H323 Encryption KeySize: <Max1024bit, Min1024bit, Min2048bit> was changed from Max1024bit to Min1024bit.
Custom wallpaper	**Bug ID: CSCvb67596** A system using custom wallpaper will not display on-screen elements for example; the clock, today's bookings or One Button to Push. This limitation is intentional as we do not know how these elements will appear on customized wallpapers. On-screen operated systems like Cisco TelePresence SX10, SX20, DX70 and DX80 are more affected by this limitation due to the lack of OBTP join mechanism compared to systems operated by a Touch 10. From CE8.3.0 a workaround was introduced to make a meeting reminder appear on-screen when the meeting starts (early reminders are not supported) to allow on-screen operated systems with custom wallpaper to join the meeting using OBTP. Note: If the reminder is dismissed the meeting must be joined manually.

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.x	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.x	

Gateway interoperability

Equipment	Software version	Comments
Cisco ISDN Link	IL1.1.6	
Cisco ISDN GW 3241	2.2	

MCU interoperability

Equipment	Software version	Comments
Cisco Meeting Server (CMS)	2.x	
Cisco TelePresence Server 7010	4.2, 4.3(x.x)	
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.x	

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.x	15.6 or later is recommended (Support for DX Series TMS management requires TMS15.3)

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 version 8 and above 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.

DX70 and DX80: http://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-command-reference-list.html

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 G2 and MX300 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		

DX70 and DX80

Compatibility level	Applicable systems	Description	Minimum software version
			CE8
0	DX70	N/A	8.2.0
0	DX80	N/A	8.2.0

Cisco TelePresence Touch 10 hardware dependencies

New hardware revisions for Cisco TelePresence Touch 10

Systems that support Touch 10 are SX10(N), SX20(N), 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
101282-0	All	N/A	8.3.3

New hardware revisions for Precision 60

Systems that support Precision 60 on CE8 are SX80, MX700, MX800 and MX800D

New hardware revisions of the Precision 60 camera are identified by production date printed on a sticker underneath the base. If there no sticker is present and you still see an error message on screen about the camera not being compatible with the current software version, please upgrade the room device to the latest software.

Production Date	Applicable systems	Description	Minimum software version
			CE8
2018/07 and earlier	All	N/A	All supported codec software versions are compatible
2018/08 and later	All	N/A	8.3.6

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
AES Encryption	s52010ce8_3_8.pkg
No Encryption	s52011cenc8_3_8.pkg
AES Encryption for CUCM	cmterm-s52010ce8_3_8.k3.cop.sgn
No Encryption for CUCM	cmterm-s52011cenc8_3_8.k3.cop.sgn

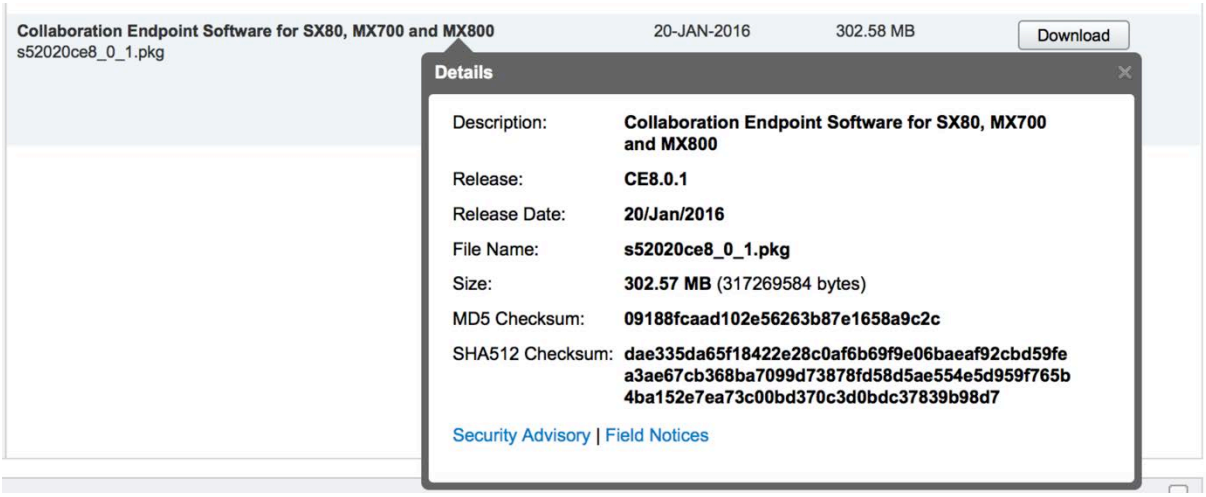
Collaboration Endpoint Software	Software for SX10	Software for MX200 G2, MX300 G2	Software for SX80, MX700, MX800, MX800 Dual	Software for DX70, DX80
Encryption and Non-encryption*	s52030ce8_3_8.pkg	s52010ce8_3_8.pkg	s52020ce8_3_8.pkg	s52040ce8_3_8.pkg
Encryption and Non-encryption* for CUCM	cmterm-s52030ce8_3_8.k3.cop.sgn	cmterm-s52010ce8_3_8.k3.cop.sgn	cmterm-s52020ce8_3_8.k3.cop.sgn	cmterm-s52040ce8_3_8.k3.cop.sgn
Encryption and Non-encryption* bundle** for CUCM	cmterm-ce8_3_8.k3.cop.sgn	cmterm-ce8_3_8.k3.cop.sgn	cmterm-ce8_3_8.k3.cop.sgn	cmterm-ce8_3_8.k3.cop.sgn

*SX10, SX80, MX700, MX800, MX800D, DX70 and DX80 do not have separate software packages for crypto and non-crypto. These systems (except DX70 and DX80) require a crypto option key to enable crypto algorithms.

** This Cisco Options Package contains a software package for all the product platforms in one file.

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_3_8.pkg SHA512
Apple MAC	Open a terminal window and type the following command $ shasum -a 512 s52020ce8_3_8.pkg

Linux	Open a terminal window and type the following command
	$ sha512sum s52020ce8_3_8.pkg
	Or
	$ shasum -a 512 s52020ce8_3_8.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.