

Collaboration Endpoint software version 8.0
NOVEMBER 2015



Administrator guide

for Cisco TelePresence SX80

Thank you for choosing Cisco!

Your Cisco product has been designed to give you many years of safe, reliable operation.

This part of the product documentation is aimed at administrators working with the setup and configuration of the video system.

Our main objective with this Administrator guide is to address your goals and needs. Please let us know how well we succeeded!

May we recommend that you visit the Cisco web site regularly for updated versions of this guide.

The user documentation can be found on

▶ <http://www.cisco.com/go/sx-docs>

How to use this guide

The top menu bar and the entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

Table of contents

Introduction	4
User documentation and software	5
What's new in CE8.0.....	6
SX80 at a glance.....	12
Power On and Off.....	13
Front panel LEDs.....	14
How to administer the video system.....	15
Configuration	19
User administration	20
Change the system passphrase	21
System configuration	22
Add a sign in banner	23
Manage the certificates of the video system.....	24
Manage the list of trusted certificate authorities (CAs)	25
Set up secure audit logging	26
Manage pre-installed certificates for CUCM via Expressway provisioning.....	27
Set strong security mode	28
Change the persistency mode.....	29
Delete CUCM trust lists.....	30
Set up Intelligent Proximity for content sharing	31
Adjust the video quality to call rate ratio.....	35
Packet loss resilience - ClearPath.....	36
Use a custom wallpaper	37
Choose ringtone	38
Manage local contacts.....	39
Peripherals	40
Connect monitors	41
Connect input sources.....	43
Set up speaker tracking	45
Set up the Snap to Whiteboard feature	46
Briefing room set-up.....	49
Real-time communication requirements for displays	52
Connect the Touch 10 controller	53
Maintenance	56
Upgrade the system software	57
Add option keys	59
System status	60

Run diagnostics.....	61
Download log files.....	62
Create a remote support user	63
Backup or restore a configuration.....	64
Revert to the previously used software image	65
Factory reset the video system	66
Factory reset the Touch 10.....	68
Capture user interface screenshots	69
System settings	70
Overview of the system settings	71
Audio settings	76
CallHistory settings	82
Cameras settings.....	83
Conference settings	88
FacilityService settings.....	93
GPIO settings.....	94
H323 settings.....	95
Logging settings	98
Network settings.....	99
NetworkServices settings.....	106
Peripherals settings	111
Phonebook settings	112
Provisioning settings.....	113
Proximity settings.....	115
RTP settings.....	116
Security settings	117
SerialPort settings.....	119
SIP settings.....	120
Standby settings	124
SystemUnit settings.....	125
Time settings	126
UserInterface settings.....	129
Video settings	131
Experimental settings	141

Appendices.....	142
How to use Touch 10	143
Set up remote monitoring	144
Access call information while using the web interface.....	145
Place a call using the web interface	146
Share content using the web interface.....	148
Local layout control.....	149
Control the local camera(s).....	150
Control the far end camera.....	151
Advanced customization of audio and GPIO.....	152
Access the video system's XML files	153
Execute API commands and configurations from the web interface	154
Manage startup scripts	155
Serial interface (RS-232)	156
Technical specification.....	157
Supported RFCs	160
User documentation on the Cisco web site.....	161
Cisco contacts	162



Chapter 1

Introduction

User documentation and software

Products covered in this guide

- Cisco TelePresence SX80

User documentation

This guide provides you with the information required to administrate the endpoint. How to install the endpoint is covered in the *Installation guide*, and the required initial configurations are described in the *Getting started guide*. Details about the codec's physical interface, including the connector panel and LEDs, are described in the *Physical interface guide*.

Refer to the ► [User documentation on the Cisco web site](#) appendix for more information about the guides for this endpoint.

Downloading the user documentation

We recommend you visit the Cisco web site regularly for updated versions of the guides:

► <http://www.cisco.com/go/sx-docs>

Software

Download software for the endpoint from the Cisco web site:

► <http://www.cisco.com/cisco/software/navigator.html>

We recommend reading the Software release notes (CE8):

► <http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/tsd-products-support-series-home.html>

What's new in CE8.0

This chapter provides an overview of the new and changed system settings, and the new features and improvements in the Cisco Collaboration Endpoint software version 8.0 (CE8.0) compared to TC7.3.

As CE software is based on TC7, the structure and main functionality remains the same as in TC software.

For more details, we recommend reading the Software release notes:

► <http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/tsd-products-support-series-home.html>

CE8.0 upgrade path



It is important to consider the upgrade requirements of CE8.0 before upgrading; otherwise upgrading to CE8.0 can leave you with a non-functioning deployment that requires you to downgrade.

Refer to the software release notes, and the

► [Upgrade the system software](#) chapter.

New features and improvements

Products

CE8.0 supports the following products:

- MX200 G2
- MX300 G2
- MX700
- MX800
- SX10 Quick Set
- SX20 Quick Set
- SX80

Cisco TelePresence products in EX Series, C Series, and Profile Series are not supported in CE software; use software version TC7.3 or earlier for these products.

User interfaces

Products running CE software, must use the following user interfaces:

- Touch 10 controller, available for all products.
- TRC6 remote control, available for SX10 and SX20.

Touch 8 controller and remote control TRC5 are not supported.

API changes

The number of API commands has been reduced. Some commands are removed, and others are different syntactically in order to cater for underlying architectural changes.

More status information and configurations are available on the video system's web interface than in the API.

Refer to the What's New chapter in the API guide for the video system, to see the changes that are made to the public API.

Intelligent Proximity for content sharing

Cisco Proximity allows you to automatically pair your device (smartphone, tablet, or laptop) with the video system when the device comes within range. This feature is disabled by default.

Cisco Proximity offers three services: Content sharing to clients, content sharing from clients and basic call control. These services are disabled by default.

The Cisco Proximity clients for smartphones and tablets (Android and iOS), and laptops (Windows and OS X) can be downloaded from ► <http://proximity.cisco.com>. Clients for smartphones and tablets are also available through Google Play (Android) and Apple App Store (iOS).

Multistream

The Multistream feature enables the video system to send and receive multiple streams of video in different resolutions simultaneously. The video systems compose layouts locally, to better adapt the layout to all available screens.

While in a conference with multiple participants, this feature enhances the user experience in terms of layout control. A multi-screen system is able to utilize all screens when participating in a Multistream enabled conference, and the layout is improved when presenting and sharing content on all systems.

In this release Multistream is switched Off by default. We recommend the Cisco UCM 11.0.0 and later, and the latest versions of TelePresence Server and TelePresenceConductor for optimal experience.

Microphone LED behaviour

The LED behavior on microphones and Touch 10 has changed. The microphone LED glows and the mute button is 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.

Resolution changes

Collaboration Endpoint Software only supports displays that support 16:9 or 16:10 resolutions.

Supports WUXGA (1920 × 1200) presentation sharing both locally and in a call.

Remote monitoring

For increased security, it is only possible to take snapshots of the local and far end video streams from the video system's web interface, when a *Remote Monitoring* option key is installed on the video system.

Remote monitoring is enabled once the option key is added, and the video system is rebooted.

No warning messages or indicators are sent to the users of the video system. Please provide adequate notice to the users that the system administrator may monitor and control the camera and screen.

Removed features

- MultiWay is no longer supported. CUCM ad hoc conferencing or hosted conferences may be used instead.
- Cisco CTMS is no longer supported. Other multipoint conferencing solutions (involving Cisco TelePresence Server, Cisco TelePresence MCU, and/or Cisco TelePresence Conductor) may be used instead.
- Custom video layouts and video composition using TC Console is not supported.
- MediaNet is no longer supported.

System configuration changes in CE8.0 compared to TC7.3

New configurations

CallHistory Mode
Conference MultiStream Mode
NetworkServices UPnP Mode
NetworkServices UPnP Timeout
Peripherals Pairing Ultrasound Volume MaxLevel
Peripherals Pairing Ultrasound Volume Mode
Proximity Mode
Proximity Services CallControl
Proximity Services ContentShare FromClients
Proximity Services ContentShare ToClients
Video DefaultMainSource

Configurations that are removed

<path> * means that all configurations starting with <path> are removed.

Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo
Audio Input HDMI [n] VideoAssociation VideoInputSource
Cameras Camera [n] DHCP
H323 Profile [1] Gatekeeper Discovery
Network [1] DHCP RequestTFTPServerAddress
NetworkServices CTMS Encryption
NetworkServices CTMS Mode
NetworkServices HTTPS Mode
NetworkServices Medianet Metadata
NetworkServices MultiWay *
SIP AuthenticateTransferror
SIP OCSP *

SIP Profile [1] Outbound
SIP Profile [1] Proxy [n] Discovery
SystemUnit CallLogging Mode
SystemUnit IrSensor
SystemUnit MenuLanguage
Time OlsonZone
UserInterface OSD LanguageSelection
UserInterface OSD LoginRequired
UserInterface TouchPanel DefaultPanel
Video AllowWebSnapshots
Video Layout DisableDisconnectedLocalOutputs
Video Layout PresentationDefault View
Video Layout ScaleToFrame
Video Layout ScaleToFrameThreshold
Video Layout Scaling
Video OSD EncryptionIndicator
Video OSD LanguageSelection
Video OSD LoginRequired
Video OSD Output
Video Wallpaper

Configurations that are modified

Cameras SpeakerTrack TrackingMode
OLD: <Default / Fast>
Default value: Default
NEW: <Auto / Conservative>
Default value: Auto

Cameras SpeakerTrack Whiteboard Mode

OLD: Required user role: ADMIN

NEW: Required user role: USER

Conference Multipoint Mode (was Conference [1] Multipoint Mode in TC7.3)

OLD: <Auto / Off / MultiSite / MultiWay / CUCMMediaResourceGroupList>

NEW: <Auto / Off / MultiSite / CUCMMediaResourceGroupList>

NetworkServices HTTP Mode

OLD: <Off / On>

Default value: On

NEW: <Off / HTTP+HTTPS / HTTPS>

Default value: HTTP+HTTPS

Phonebook Server[n] Type

OLD: <VCS / TMS / Callway / CUCM>

Default value: TMS

NEW: <Off / VCS / TMS / CUCM>

Default value: Off

Provisioning Mode

OLD: <Off / TMS / VCS / Callway / CUCM / Auto / Edge>

NEW: <Off / TMS / VCS / CUCM / Auto / Edge>

Standby BootAction

OLD: <None / Preset1 / Preset2 / Preset3 / Preset4 / Preset5 / Preset6 / Preset7 / Preset8 / Preset9 / Preset10 / Preset11 / Preset12 / Preset13 / Preset14 / Preset15 / RestoreCameraPosition / DefaultCameraPosition>

NEW: <None / RestoreCameraPosition / DefaultCameraPosition>

Standby WakeupAction

OLD: <None / Preset1 / Preset2 / Preset3 / Preset4 / Preset5 / Preset6 / Preset7 / Preset8 / Preset9 / Preset10 / Preset11 / Preset12 / Preset13 / Preset14 / Preset15 / RestoreCameraPosition / DefaultCameraPosition>

NEW: <None / RestoreCameraPosition / DefaultCameraPosition>

Time Zone

Change: The list of time zones is updated. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Video DefaultLayoutFamily Local (was Video Layout LocalLayoutFamily in TC7.3)

OLD: <Auto / FullScreen / Equal / PresentationSmallSpeaker / PresentationLargeSpeaker / Prominent / Overlay / Single>

NEW: <Auto / Equal / Prominent / Overlay / Single>

Video DefaultLayoutFamily Remote (was Video Layout RemoteLayoutFamily in TC7.3)

OLD: <Auto / FullScreen / Equal / PresentationSmallSpeaker / PresentationLargeSpeaker / Prominent / Overlay / Single>

NEW: <Auto / Equal / Prominent / Overlay / Single>

Video Input Connector [n] InputSourceType

OLD: <other / camera / PC / DVD / document_camera / whiteboard>

NEW: <other / camera / PC / mediaplayer / document_camera / whiteboard>

Video Input Connector [n] PresentationSelection

OLD: <Manual / Automatic / OnConnect>

NEW: <Manual / OnConnect>

Video Output Connector [n] MonitorRole

OLD: <Auto / First / Second / PresentationOnly / Third >

NEW: <Auto / First / Second / PresentationOnly / Third / Recorder>

Video Output Connector [n] Resolution

OLD: <Auto / 1280_720_50 / 1280_720_60 / 1920_1080_50 / 1920_1080_60>

NEW: <Auto / 1280_720_50 / 1280_720_60 / 1920_1080_50 / 1920_1080_60 / 1920_1200_50 / 1920_1200_60>

Configurations that are renamed

Audio SoundsAndAlerts KeyTones Mode

Renamed to: UserInterface KeyTones Mode

Cameras Camera [n] Backlight

Renamed to: Cameras Camera [n] Backlight DefaultMode

Cameras Camera [n] Brightness Level

Renamed to: Cameras Camera [n] Brightness DefaultLevel

Conference [1] ActiveControl Mode

Renamed to: Conference ActiveControl Mode

Conference [1] AutoAnswer Delay

Renamed to: Conference AutoAnswer Delay

Conference [1] AutoAnswer Mode

Renamed to: Conference AutoAnswer Mode

Conference [1] AutoAnswer Mute

Renamed to: Conference AutoAnswer Mute

Conference [1] CallProtocollPStack

[Renamed to:](#) Conference CallProtocollPStack

Conference [1] DefaultCall Protocol

[Renamed to:](#) Conference DefaultCall Protocol

Conference [1] DefaultCall Rate

[Renamed to:](#) Conference DefaultCall Rate

Conference [1] DoNotDisturb DefaultTimeout

[Renamed to:](#) Conference DoNotDisturb DefaultTimeout

Conference [1] Encryption Mode

[Renamed to:](#) Conference Encryption Mode

Conference [1] FarEndControl Mode

[Renamed to:](#) Conference FarEndControl Mode

Conference [1] FarEndControl SignalCapability

[Renamed to:](#) Conference FarEndControl SignalCapability

Conference [1] IncomingMultisiteCall Mode

[Renamed to:](#) Conference IncomingMultisiteCall Mode

Conference [1] MaxReceiveCallRate

[Renamed to:](#) Conference MaxReceiveCallRate

Conference [1] MaxTotalReceiveCallRate

[Renamed to:](#) Conference MaxTotalReceiveCallRate

Conference [1] MaxTotalTransmitCallRate

[Renamed to:](#) Conference MaxTotalTransmitCallRate

Conference [1] MaxTransmitCallRate

[Renamed to:](#) Conference MaxTransmitCallRate

Conference [1] MicUnmuteOnDisconnect Mode

[Renamed to:](#) Conference MicUnmuteOnDisconnect Mode

Conference [1] Multipoint Mode

[Renamed to:](#) Conference Multipoint Mode

Conference [1] Presentation OnPlacedOnHold

[Renamed to:](#) Conference Presentation OnPlacedOnHold

Conference [1] Presentation RelayQuality

[Renamed to:](#) Conference Presentation RelayQuality

Conference [1] VideoBandwidth MainChannel Weight

[Renamed to:](#) Conference VideoBandwidth MainChannel Weight

Conference [1] VideoBandwidth Mode

[Renamed to:](#) Conference VideoBandwidth Mode

Conference [1] VideoBandwidth PresentationChannel Weight

[Renamed to:](#) Conference VideoBandwidth PresentationChannel Weight

H323 Profile [1] Authentication LoginName

[Renamed to:](#) H323 Authentication LoginName

H323 Profile [1] Authentication Mode

[Renamed to:](#) H323 Authentication Mode

H323 Profile [1] Authentication Password

[Renamed to:](#) H323 Authentication Password

H323 Profile [1] CallSetup Mode

[Renamed to:](#) H323 CallSetup Mode

H323 Profile [1] Encryption KeySize

[Renamed to:](#) H323 Encryption KeySize

H323 Profile [1] Gatekeeper Address

[Renamed to:](#) H323 Gatekeeper Address

H323 Profile [1] H323Alias E164

[Renamed to:](#) H323 H323Alias E164

H323 Profile [1] H323Alias ID

[Renamed to:](#) H323 H323Alias ID

H323 Profile[1] PortAllocation

[Renamed to:](#) H323 PortAllocation

NetworkServices NTP Address

[Renamed to:](#) NetworkServices NTP Server [n] Address

SIP Profile [1] Authentication [1] LoginName

[Renamed to:](#) SIP Authentication UserName

SIP Profile [1] Authentication [1] Password

[Renamed to:](#) SIP Authentication Password

SIP Profile [1] DefaultTransport

[Renamed to:](#) SIP DefaultTransport

SIP Profile [1] DisplayName
[Renamed to:](#) SIP DisplayName

SIP Profile [1] Ice DefaultCandidate
[Renamed to:](#) SIP Ice DefaultCandidate

SIP Profile [1] Ice Mode
[Renamed to:](#) SIP Ice Mode

SIP Profile[1] Line
[Renamed to:](#) SIP Line

SIP Profile[1] Mailbox
[Renamed to:](#) SIP Mailbox

SIP Profile [1] Proxy [n] Address
[Renamed to:](#) SIP Proxy [n] Address

SIP Profile [1] TlsVerify
[Renamed to:](#) SIP TlsVerify

SIP Profile [1] Turn BandwidthProbe
[Renamed to:](#) SIP Turn BandwidthProbe

SIP Profile [1] Turn DiscoverMode
[Renamed to:](#) SIP Turn DiscoverMode

SIP Profile [1] Turn DropRflx
[Renamed to:](#) SIP Turn DropRflx

SIP Profile [1] Turn Password
[Renamed to:](#) SIP Turn Password

SIP Profile [1] Turn Server
[Renamed to:](#) SIP Turn Server

SIP Profile [1] Turn UserName
[Renamed to:](#) SIP Turn UserName

SIP Profile [1] Type
[Renamed to:](#) SIP Type

SIP Profile [1] URI
[Renamed to:](#) SIP URI

SystemUnit ContactInfo Type
[Renamed to:](#) UserInterface ContactInfo Type

Video CamCtrlPip CallSetup Duration
[Renamed to:](#) Video Selfview OnCall Duration

Video CamCtrlPip CallSetup Mode
[Renamed to:](#) Video Selfview OnCall Mode

Video DefaultPresentationSource
[Renamed to:](#) Video Presentation DefaultSource

Video Layout LocalLayoutFamily
[Renamed to:](#) Video DefaultLayoutFamily Local

Video Layout RemoteLayoutFamily
[Renamed to:](#) Video DefaultLayoutFamily Remote

Video PIP ActiveSpeaker DefaultValue Position
[Renamed to:](#) Video ActiveSpeaker DefaultPIPPosition

Video PIP Presentation DefaultValue Position
[Renamed to:](#) Video Presentation DefaultPIPPosition

Video SelfviewDefault FullscreenMode
[Renamed to:](#) Video Selfview Default FullscreenMode

Video SelfviewDefault Mode
[Renamed to:](#) Video Selfview Default Mode

Video SelfviewDefault OnMonitorRole
[Renamed to:](#) Video Selfview Default OnMonitorRole

Video SelfviewDefault PIPPosition
[Renamed to:](#) Video Selfview Default PIPPosition

SX80 at a glance

The Cisco TelePresence SX80 codec provides a powerful and flexible platform for creating video collaboration experiences. SX80 was built with the integrator in mind, enabling flexibility and creativity for customized video collaboration rooms. SX80 acts as the audio and video engine to incorporate high-definition video collaboration applications into large meeting rooms, boardrooms and purpose-built or vertical application rooms.

SX80 delivers up to a 1080p60 end-to-end high definition (HD) video and offers industry-first support for H.265 (in SIP calls). The codec offers a rich input and output set, flexible media engine, and support for three screens enable various use cases.

Cisco offers SX80 as a single unit, and in the following integrator packages:

- SX80 and Precision 40 (PrecisionHD 1080p4xS2) camera for smaller room scenarios
- SX80 and Precision 60 camera, for larger room scenarios with premium image quality
- SX80 and SpeakerTrack 60 dual camera system, which features a direct, fast switching approach for active speaker tracking

SX80 also has basic support for the PrecisionHD 1080p12x camera (camera software upgrade not supported natively by codec, Daisy chaining not supported).

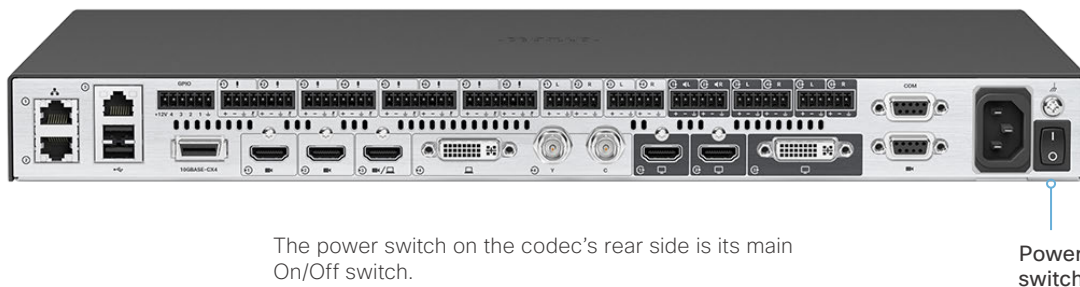


Features and benefits

- The codec is compatible with standards-based video systems without loss of features.
- Operation using Cisco TelePresence Touch 10 user interface, or with an external control device using the API (no IR and remote control).
- Simple *one-button-to-push* to join scheduled meetings.
- Embedded MultiSite conferencing option that allows up to four additional participants (individual transcoding, no external bridge).
- Cisco TelePresence ClearPath packet loss protection technology.
- Cisco Unified Communications Manager (CUCM) native support. Requires CUCM version 8.6 or higher.
- The systems support H.323 and SIP with bandwidth up to 6 Mbps point-to-point.
- Up to 6 Mbps total MultiSite bandwidth.
- Full duplex audio with high-quality stereo sound.
- Video resolution and frame rate up to 1080p60.
- Support for 1080p30 content and 1080p60 video simultaneously.
- Full application programming interface (API).
- Ability to connect up to four HD sources and eight microphones.
- Ability to connect to up to three monitors or output devices.
- Professional-grade connectors.
- One rack unit (1RU) high, rack-mountable.

Power On and Off

Power On/Off with the Power switch or Shutdown button



The power switch on the codec's rear side is its main On/Off switch.

It may take a few minutes for the codec to start up. The system is ready for use when the Power LED lights steadily.



Shutdown button

You can use the Shutdown button on the front panel to switch the codec On/Off, provided that the Power switch on the codec's rear side is On.

- To switch Off the codec, hold the button until the LEDs go out.
- To switch On the codec, hold the button until the LEDs flash. It may take a few minutes for the codec to start up. The system is ready for use when the Power LED lights steadily.

Power Off or restart the system remotely

Sign in to the web interface and navigate to [Maintenance > Restart](#).

Restart the system

Click [Restart TelePresence device...](#) and confirm your choice.

- i** It will take a few minutes before the system is ready for use.

Power Off the system

Click [Shutdown TelePresence device...](#) and confirm your choice.

- i** The system cannot be powered On again remotely.

Front panel LEDs



Front panel LEDs

Power:

- Blinks when the system is starting up.
- Steady light when the codec is ready for use.
- Pulsates when the codec is in standby.

In Call:


- Steady light when in call.

IR:

- Not in use.

Alarm:

- Lights steady when a serious error occurs.

 More information about the codec's physical interface, including the connector panel and LEDs, are described in the *Physical interface guide*.

How to administer the video system (page 1 of 4)

In general, we recommend you to use the web interface to administer and maintain the video system, as described in this administrator guide.

Alternatively, you can access the API of the video system by other methods:

- HTTP or HTTPS (also used by the web interface)
- SSH
- Telnet
- Serial interface (RS-232)

If you want more information about the different access methods, and how to use the API, refer to the *API guide* for the video system.

Tip

If the configuration or status is available in the API, the web interface setting or status translates into an API configuration or status as follows:

Set `X > Y > Z` to **Value** (web)
is the same as
`xConfiguration X Y Z: Value` (API)

Check `X > Y > Z` status (web)
is the same as
`xStatus X Y Z` (API)

For example:

Set `SystemUnit > Name` to **MySystem**
is the same as
`xConfiguration SystemUnit Name: MySystem`

Check `SystemUnit > Software > Version` status
is the same as
`xStatus SystemUnit Software Version`

More settings and status are available in the web interface than in the API.

Access method	Notes	How to enable/disable the methods
HTTP/HTTPS	<ul style="list-style-type: none"> • Used by the web interface of the video system • Nonsecure (HTTP) or secure (HTTPS) communication • HTTP: <i>Enabled</i> by default • HTTPS: <i>Enabled</i> by default 	<p>NetworkServices > HTTP > Mode</p> <p>Restart the video system for changes to take effect</p>
Telnet	<ul style="list-style-type: none"> • Nonsecure TCP/IP connection • <i>Disabled</i> by default 	<p>NetworkServices > Telnet > Mode</p> <p>You do not need to restart the video system. It may take some time for changes to take effect</p>
SSH	<ul style="list-style-type: none"> • Secure TCP/IP connection • <i>Enabled</i> by default 	<p>NetworkServices > SSH > Mode</p> <p>You do not need to restart the video system. It may take some time for changes to take effect</p>
Serial interface (RS-232)	<ul style="list-style-type: none"> • Connect to the video system with a cable. IP-address, DNS, or a network is not required • <i>Enabled</i> by default • We recommend using the default baud rate, because the video system may return much feedback (SerialPort > BaudRate) • For security reasons, you are asked to sign in by default (SerialPort > LoginRequired) 	<p>SerialPort > Mode</p> <p>Restart the video system for changes to take effect</p>



If all access methods are disabled (set to **Off**), you can no longer configure the video system. You are not able to reenable (set to **On**) any of the access methods, and you must factory reset the video system to recover.

How to administer the video system (page 2 of 4)

The web interface of the video system

The web interface is the administration portal for the video system. You can connect from a computer and administer the system remotely. It provides full configuration access and offers tools and mechanisms for maintenance.

Note: The web interface requires that HTTP or HTTPS is enabled (refer to [NetworkServices > HTTP > Mode](#) setting).

We recommend that you use the latest release of one of the major web browsers.

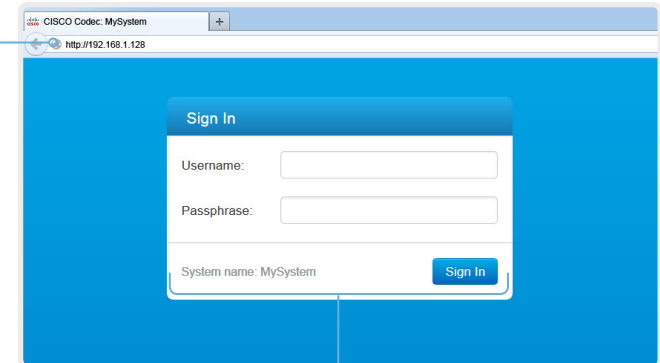
Connect to the video system

Open a web browser and enter the IP address of the video system in the address bar.



How to find the IP address

Tap the contact information in the upper left corner of the Touch controller. Then tap [Settings > System Information](#).



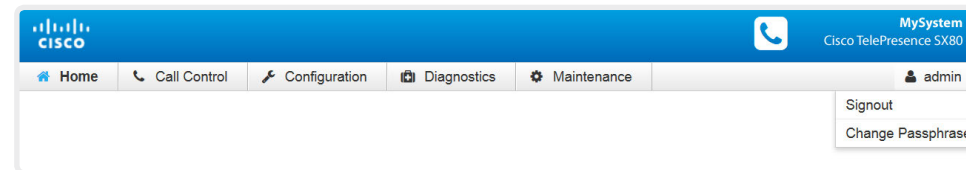
Sign in

Enter user name and passphrase for the endpoint and click [Sign In](#).



The system is delivered with a default user named *admin* with no passphrase. Leave the [Passphrase](#) field blank when signing in for the first time.

It is mandatory to set a password for the *admin* user.



Sign out

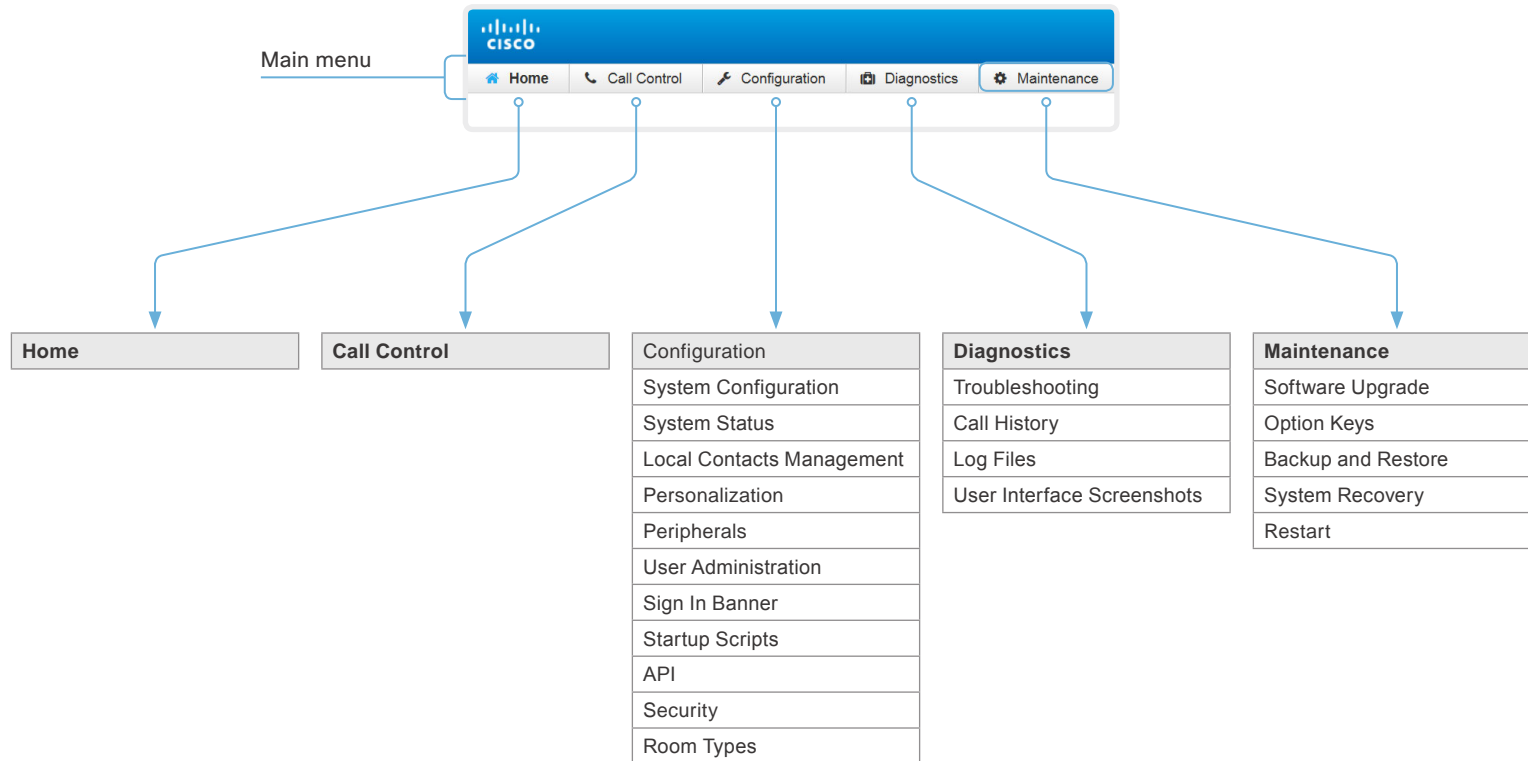
Hover the mouse over the user name and choose [Signout](#) from the drop-down list.

How to administer the video system (page 3 of 4)

How the web interface is organized

The web interface is organized in sub-pages. A user that is signed in, sees only the pages that he has access rights for.

Read more about user administration, user roles and access rights in the [User administration](#) chapter.



How to administer the video system (page 4 of 4)

Settings available on the Touch controller

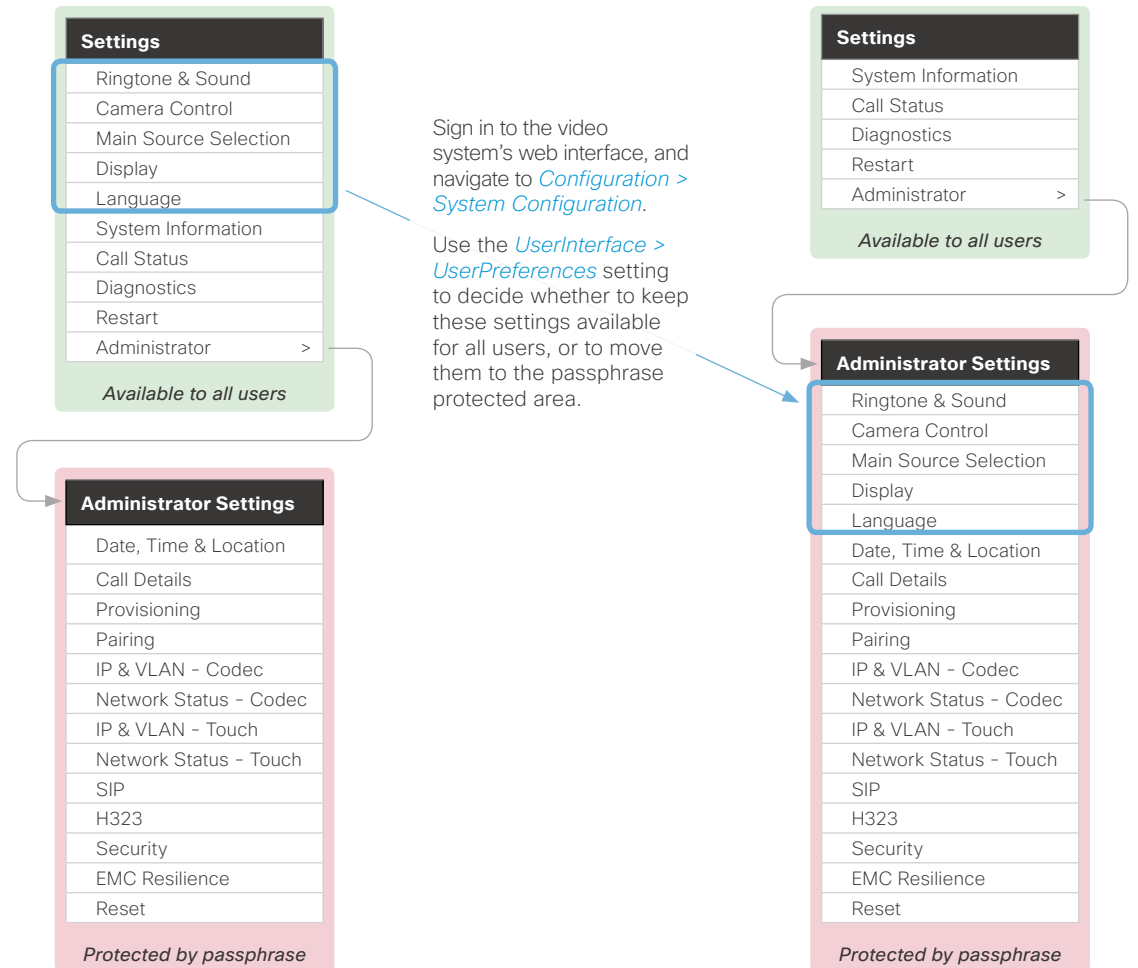
You can access the following information and settings on the Touch controller:

- System information, call status, and diagnostics (available to all users)
- Restart of the video system (available to all users)
- Basic settings for sound, camera, main source, display, language (may or may not be protected by passphrase, refer to the [UserInterface > UserPreferences](#) setting)
- Basic settings for pairing, provisioning, network, IP and call protocols (always protected by passphrase)

Access Settings

1. Tap the contact information in the upper left corner of the Touch controller.
2. Tap [Settings](#).
3. Choose a category in the list*.

You have to enter the *Username* and *Passphrase* of the video system to open the [Administrator](#) settings.



[UserInterface > UserPreferences](#): On (default)

[UserInterface > UserPreferences](#): Off

* Depending on product and product set-up, your Touch controller may or may not display the same menus as shown in the illustration.



Chapter 2

Configuration

User administration

The default user account

The endpoint comes with a default administrator user account with full access rights. The user name is *admin* and no passphrase is initially set.

 It is mandatory to set a passphrase for the *admin* user.

Read how to set the passphrase in the [► Change the system passphrase](#) chapter.

Create a new user account

1. Sign in to the web interface, and navigate to [Configuration > User Administration](#).

2. Click [Add new user...](#)

3. Fill in the Username and Passphrase* input fields, and check the appropriate user roles check boxes.

As a default, the user has to change the passphrase when he signs in for the first time.

Fill in the Client Certificate DN (Distinguished Name) field only if you use certificate login on HTTPS.

4. Set the Status to **Active** to activate the user.

5. Click [Create User](#).

Use the [Back](#) button to leave without making any changes.

* The passphrase protects the web and command line interfaces, and the Administrator settings on the Touch controller.

Edit an existing user account

Change the user privileges

1. Sign in to the web interface, and navigate to [Configuration > User Administration](#).
2. Click the appropriate user in the list.
3. Choose user roles, set the status to Active or Inactive, and decide if the user has to change the passphrase on the next sign in.

Fill in the Client Certificate DN (Distinguished Name) field only if you use certificate login on HTTPS.

4. Click [Update User](#) to save the changes.
Use the [Back](#) button to leave without making any changes.

Change the passphrase

1. Sign in to the web interface, and navigate to [Configuration > User Administration](#).
2. Click the appropriate user in the list.
3. Enter the new passphrase in the appropriate input fields.
4. Click [Change Passphrase](#) to save the change.
Use the [Back](#) button to leave without making any changes.

Delete the user account

1. Sign in to the web interface, and navigate to [Configuration > User Administration](#).
2. Click the appropriate user in the list.
3. Click [Delete <user name>...](#) and confirm when prompted.

About user roles

A user account may hold one or a combination of *user roles*.

The user roles have *non-overlapping rights*.

ADMIN: A user with this role can create new users and change most settings. The user cannot upload audit certificates and change the security audit settings.

USER: A user with this role can make calls and search the contact lists. The user can modify a few settings, for example adjust the ringtone volume and set the time and date format.

AUDIT: A user with this role can change the security audit settings and upload audit certificates.

Note that an administrator user account with full access rights, like the default *admin* user, must possess all roles.


Change the system passphrase

You need to know the system passphrase in order to:

- Sign in to the web interface
- Sign in and use the command line interfaces
- Access the Administrator settings from a Touch controller

The default user account

The video system is delivered with a default user account with full access rights. The user name is *admin*, and initially, no passphrase is set.

 It is mandatory to set a passphrase for the default *admin* user in order to restrict access to system configuration. It is also mandatory to set a passphrase for any other user with ADMIN rights.

Keep a copy of the passphrase in a safe place. You have to factory reset the unit if you forget the passphrase.

A warning, saying that the system passphrase is not set, is shown on screen until a passphrase is set for the *admin* user.

Other user accounts


You can create many user accounts for the video system.

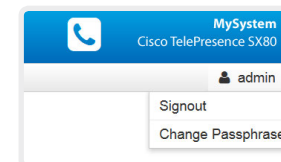
Read more about how to create and manage user accounts in the [User administration](#) chapter.

Change your passphrase

1. Sign in to the web interface, hover the mouse over the user name, and choose [Change Passphrase](#) in the drop down list.
2. Enter the current passphrase and new passphrase in the input fields, and click [Change passphrase](#).

The passphrase format is a string with 0–64 characters.

 If the passphrase currently is not set, leave the [Current passphrase](#) field blank.



Change another user's passphrase

If you have administrator access rights, you can change the password of any user.

1. Sign in to the web interface, and navigate to [Configuration > User Administration](#).
2. Click the appropriate user in the list.
3. Enter the new passphrase in the appropriate input fields.
4. Click [Change Passphrase](#) to save the change.

Use the [Back](#) button to leave without making any changes.

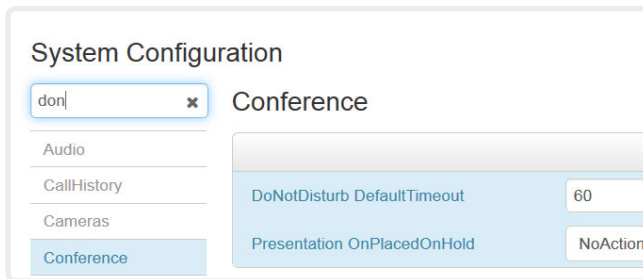
System configuration

Sign in to the web interface, and navigate to [Configuration > System Configuration](#).

Find a system setting

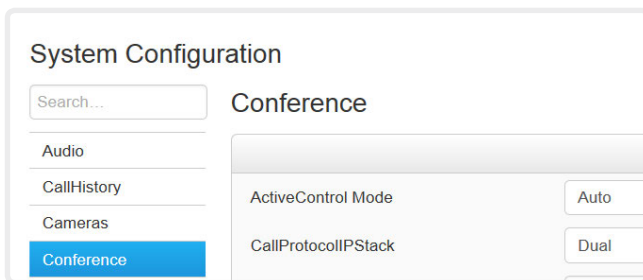
Search for settings

Enter as many letters as needed in the search field. All settings that contain these letters are shown in the right pane. Settings that have these letters in their value space are also shown.



Select a category and navigate to settings

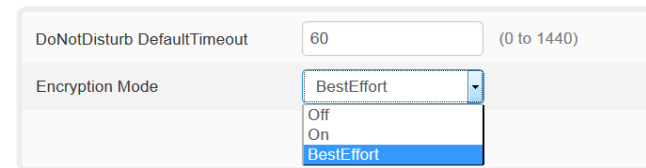
The system settings are grouped in categories. Choose a category in the left pane to show the associated settings.



Change a system setting

Check the value space

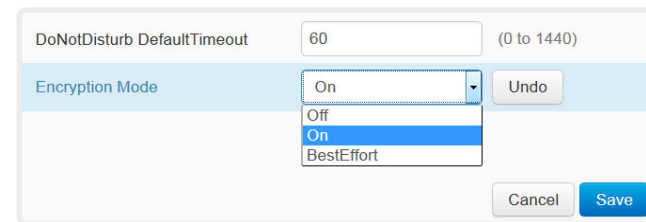
A settings's value space is specified either by text following the input field or in a drop-down list that opens when you click the arrow.



Change a value

1. Choose the preferred value from the drop-down list, or enter new text in the input field.
2. Click [Save](#) for the change to take effect.

Use the [Undo](#) or [Cancel](#) buttons if you do not want to make any changes.



Categories with unsaved changes are marked with an edit symbol (✎).

About system settings

All system settings can be changed from the web interface.

Each system setting is described in the [System settings](#) chapter.

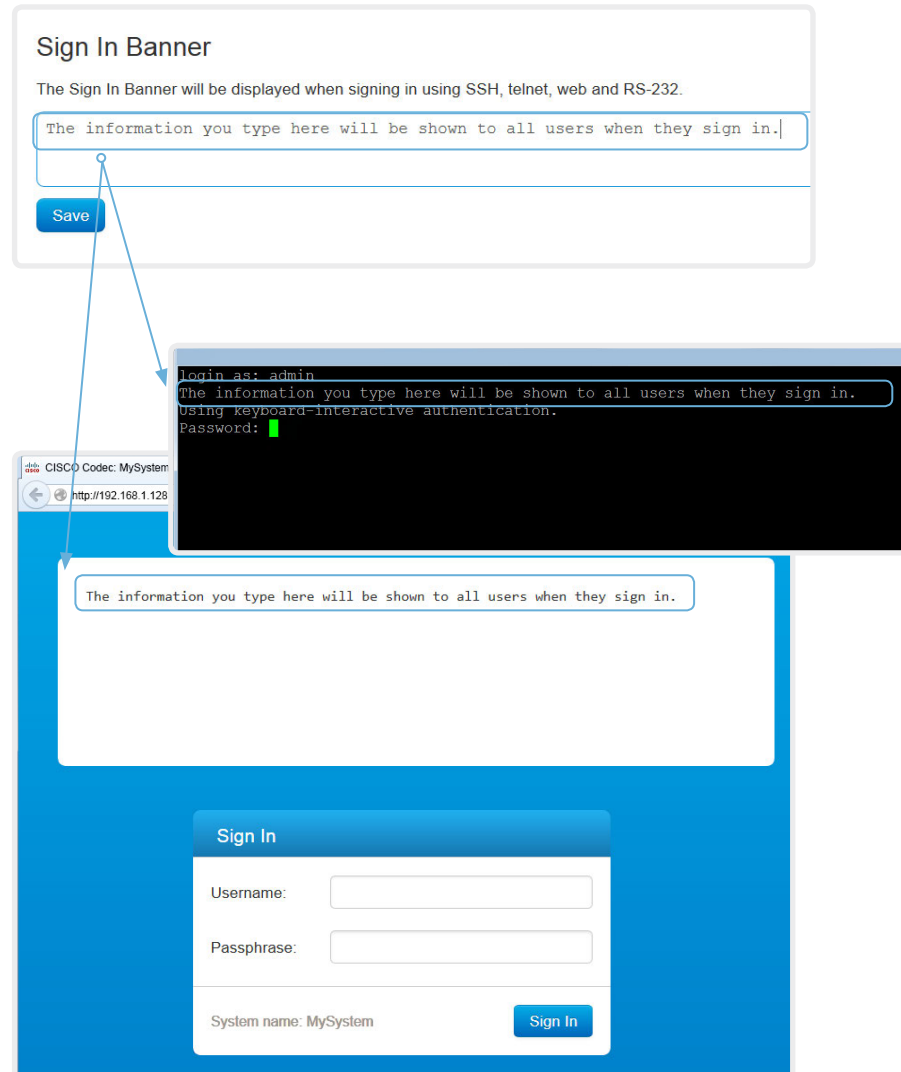
Different settings may require different user credentials. In order to be sure that an administrator is able to change all system settings, an administrator user must possess all user roles.

You can read more about user administration and user roles in the [User administration](#) chapter.

Add a sign in banner

Sign in to the web interface, and navigate to [Configuration > Sign In Banner](#).

1. Enter the message that you want to present to the user when he signs in.
2. Click [Save](#) to activate the banner.



About sign in banner

If a system administrator wants to provide initial information to all users, he can create a sign in banner. The message will be shown when the user signs in to the web interface or the command line interface.

Manage the certificates of the video system

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [Certificates](#) tab.

You need the following files:

- Certificate (file format: .PEM)
- Private key, either as a separate file or included in the same file as the certificate (file format: .PEM format)
- Passphrase (required only if the private key is encrypted)

The certificate and the private key will be stored in the same file on the video system.

About the certificates of the video system

Certificate validation may be required when using TLS (Transport Layer Security).

A server or client may require that the video system presents a valid certificate to them before communication can be set up.

The video system's certificates are text files that verify the authenticity of the system. These certificates may be issued by a certificate authority (CA).

Certificates are used for the following services: HTTPS server, SIP, IEEE 802.1X and audit logging.

You can store many certificates on the video system, but only one certificate can be enabled for each service at a time.

If authentication fails, the connection will not be established.

Enable or disable, view or delete a certificate

Use the On/Off buttons to enable or disable a certificate for the different services.

Use the corresponding button to view or delete a certificate.

Certificate	Issuer	HTTPS server	SIP	802.1X	Audit log		
Certificate_A	CertificateAuthority_A	On	Off	Off	Off	Delete...	View Certificate
Certificate_B	CertificateAuthority_B	Off	Off	Off	Off	Delete...	View Certificate

Add Certificate

Certificate No file selected.

Private key (optional) No file selected.

Passphrase (optional)

This system supports PEM formatted certificate files (.pem). The certificate file may contain the certificate and a RSA or DSA encrypted private key with or without a passphrase. Optionally the private key file may be supplied separately.

The certificates and certificate issuers in the illustration are examples. Your system has other certificates.

Add a certificate

1. Click [Browse...](#) and find the Certificate file and Private key file (optional) on your computer.
2. Fill in the [Passphrase](#) if required.
3. Click [Add certificate...](#) to store the certificate on the video system.

Manage the list of trusted certificate authorities (CAs)

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [CAs](#) tab.

You need the following file:

- CA certificate list (file format: .PEM).

View or delete a certificate

Use the corresponding button to view or delete a certificate.

Upload a list of certificate authorities

1. Click [Browse...](#) and find the file containing a list of CA certificates on your computer (file format: .PEM).
2. Click the [Add certificate authority...](#) to store the new CA certificates on the video system.

The certificates and certificate issuers in the illustration are examples. Your system has other certificates.



Previously stored certificates are not deleted automatically.

The entries in a new file with CA certificates are appended to the existing list.

About trusted CAs

Certificate validation may be required when using TLS (Transport Layer Security).

The video system may be set up to require that a server or client presents its certificate to the video system before communication can be set up.

The certificates are text files that verify the authenticity of a server or client. The certificates must be signed by a trusted CA.


In order to verify the signature of the certificates, a list of trusted CAs must reside on the video system.

The list must include all CAs needed in order to verify certificates for both audit logging and other connections.

If authentication fails, the connection will not be established.

Set up secure audit logging

Sign in to the web interface, navigate to [Configuration > System Configuration](#).

 The certificate authority (CA) that verifies the certificate of the audit server must be in the video system's list of trusted certificate authorities. Otherwise, logs will not be sent to the external server.

Refer to the [Manage the list of trusted certificate authorities \(CAs\)](#) chapter how to update the list.

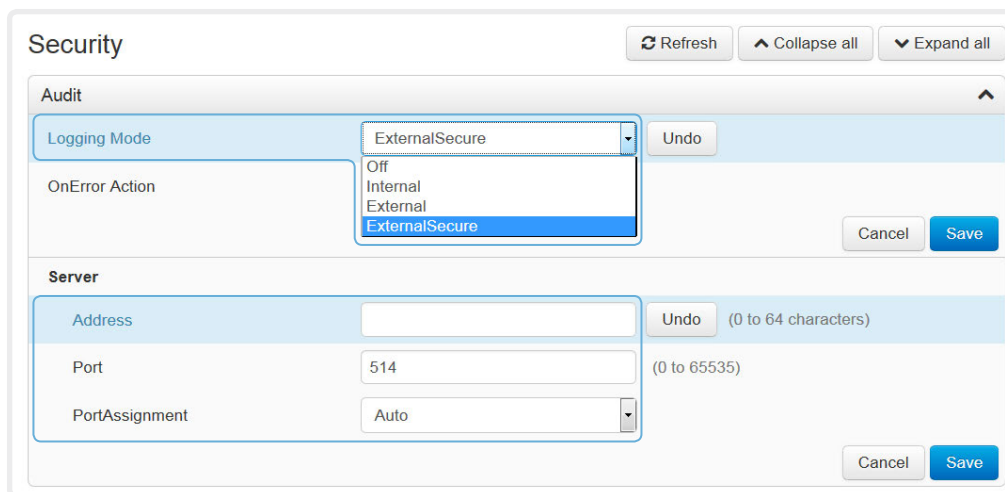
1. Open the [Security](#) category.
2. Find the [Audit > Server](#) settings, and enter the [Address](#) of the audit server.

If you set [PortAssignment](#) to **Manual**, you must also enter a [Port](#) number for the audit server.

Click [Save](#) for the changes to take effect.

3. Set [Audit > Logging Mode](#) to **ExternalSecure**.

Click [Save](#) for the change to take effect.



The screenshot shows the 'Security' configuration page with two main sections: 'Audit' and 'Server'.
 In the 'Audit' section, the 'Logging Mode' dropdown is set to 'ExternalSecure', with a list of options (Off, Internal, External, ExternalSecure) visible. There is an 'Undo' button next to it. The 'OnError Action' field is empty.
 In the 'Server' section, the 'Address' field is empty with an 'Undo' button and a note '(0 to 64 characters)'. The 'Port' field contains '514' with a note '(0 to 65535)'. The 'PortAssignment' dropdown is set to 'Auto'.
 Both sections have 'Cancel' and 'Save' buttons at the bottom right.

About secure audit logging

When audit logging is enabled, all sign in activity and configuration changes on the video system are recorded.

Use the [Security > Audit > Logging Mode](#) setting to enable audit logging. Audit logging is disabled by default.

In ExternalSecure audit logging mode the video system sends encrypted audit logs to an external audit server (syslog server), which identity must be verified by a signed certificate.

The signature of the audit server is verified using the same CA list as other servers/clients.

If the audit server authentication fails, no audit logs are sent to the external server.

Manage pre-installed certificates for CUCM via Expressway provisioning

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [Preinstalled CAs](#) tab.

Security

Preinstalled CAs

This CA list is used for Cisco UCM via Expressway (Edge) provisioning only.

[Configure provisioning now.](#)

These certificates are used to validate the servers contacted over the Internet when the endpoint uses Cisco UCM via Expressway provisioning.

Certificate	Issuer		
Certificate_01	Issuer_1	Details...	Disable
Certificate_02	Issuer_2	Details...	Disable
Certificate_03	Issuer_3	Details...	Disable

Disable All

View or disable certificates

Use the [Details...](#) and [Disable](#) buttons respectively, to view or disable certificates.



As an alternative to using the pre-installed certificates, you can append the certificate you need to the certificate list manually.

Refer to the [Manage the list of trusted certificate authorities \(CAs\)](#) chapter how to update the list of trusted certificates.

About pre-installed certificates

The pre-installed certificates in this list are only used when the video system is provisioned by Cisco Unified Communications Manager (CUCM) via Expressway (Edge).

Only Cisco Expressway infrastructure certificates are checked against this list.

If the validation of the Cisco Expressway infrastructure certificate fails, the video system will not be provisioned and registered.

Factory resetting the video system does not delete the list of pre-installed certificates.

Set strong security mode

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [Strong Security Mode](#) tab.

Set strong security mode

Read carefully about the consequences of strong security mode before you continue.

1. If you want to use strong security mode, click [Enable strong security mode...](#) and confirm your choice in the dialog box that appears.
The video system restarts automatically.
2. Change the passphrase when you are prompted. The new passphrase must meet the strict criteria as described.

How to change the system passphrase is described in the [Change the system passphrase](#) chapter.

Return to normal mode

Click [Disable strong security mode...](#) in order to restore the video system to normal mode. Confirm your choice in the dialog box that appears.

The video system restarts automatically.

Security

Strong Security Mode

Strong Security Mode is **not** enabled.

Strong Security Mode is required to adhere to U.S. Department of Defense JITC regulations.

It will introduce the following:

- All users and administrators must change their passphrase and PIN on the next sign in
- New passphrases must meet the following criteria:
 - Minimum 15 characters
 - Minimum 2 uppercase alphabetic characters
 - Minimum 2 lowercase alphabetic characters
 - Minimum 2 numerical characters
 - Minimum 2 non-alphanumeric (special) characters
 - No more than 2 consecutive characters may be the same
 - Must be different from the last 10 previous passphrases used
 - Not more than 2 characters from the previous passphrase can be in the same position
- Passphrases must be changed at least every 60 days
- Passphrases cannot be changed more than once per 24 hours
- 3 failed signins will lock the user account until an administrator re-activates the account

[Enable Strong Security Mode...](#)

Security

Certificates Strong Security Mode

Strong Security Mode is enabled.

[Disable Strong Security Mode...](#)

About strong security mode

Use strong security mode only when compliance with DoD JITC regulations is required.

Strong security mode sets very strict passphrase requirements, and requires all users to change their passphrase on the next sign in.

Change the persistency mode

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [Non-persistent Mode](#) tab.

Check the persistency status

The active radio buttons show the current persistency status of the video system.

Alternatively, navigate to [Configuration > System Status > Security > Persistency](#) to see the status.

Change the persistency settings

1. Click the radio buttons to set the persistency for configurations, call history, internal logging, local phonebook (local directory and favorites) and IP connectivity (DHCP) information.
2. Click [Save and reboot...](#)

The video system restarts automatically. After the restart, the behavior changes according to the new persistency settings.



Logs, configurations and other data that was stored before the switch to Non-persistent mode, are NOT cleared or deleted.

About persistency mode

By default, all persistency settings are set to **Persistent**. This means that configurations, call history, internal logs, local phonebook (local directory and favorites list) and IP connectivity information are stored as normal. A system restart does not delete this information.

As a general rule, we recommend NOT to change the default settings for persistency. **Non-persistent** mode must be used in situations where a user is not supposed to see or trace back to any kind of logged information from the previous session.

In Non-persistent mode, the following information is lost or cleared each time the system restarts:

- System configuration changes
- Information about calls that are placed or received (call history)
- Internal log files
- Changes to the local contacts or favorites list
- All IP related information (DHCP) from the last session



In order to clear/delete information that was stored before changing to Non-persistent mode, you should factory reset the video system.

There is more information about performing a factory reset in the [▶ Factory reset the video system](#) chapter.


Delete CUCM trust lists

The information in this chapter is only relevant for video systems that are registered to a Cisco Unified Communications Manager (CUCM).

Sign in to the web interface, navigate to [Configuration > Security](#), and open the [CUCM](#) tab.

Delete the CUCM trust lists

Click [Delete CTL/ITL](#) to remove the trust lists.

 As a general rule, you should not delete old CTL (Certificate Trust List) and ITL (Initial Trust List) files.

In these cases, you must still delete them:

- When you change the CUCM IP address.
- When you move the endpoint between CUCM clusters.
- When you need to re-generate or change the CUCM certificate.

Overview of trust list fingerprints and certificates

The trust lists' fingerprints and an overview of the certificates in the lists are displayed on the web page.

This information may be useful for troubleshooting.

More information about trust lists

For more information about CUCM and trust lists, read the *Deployment guide for TelePresence endpoints on CUCM* that is available on the Cisco web site.

Set up Intelligent Proximity for content sharing (page 1 of 4)

Cisco Proximity allows users to see, control, capture and share content directly on their own mobile devices (smartphone, tablet, or laptop), when the device is near a video system.

The mobile device can automatically pair with the video system when it comes within range of ultrasound transmitted by the video system.



The number of simultaneous Proximity connections depends on the type of video system. The client warns new users if the maximum number of connections has been reached.

Video system	Maximum number of connections
SX80	10
SX20	7
SX10	7
MX700, MX800	10
MX200 G2, MX300 G2	7

Proximity services

Place calls and control the video system:

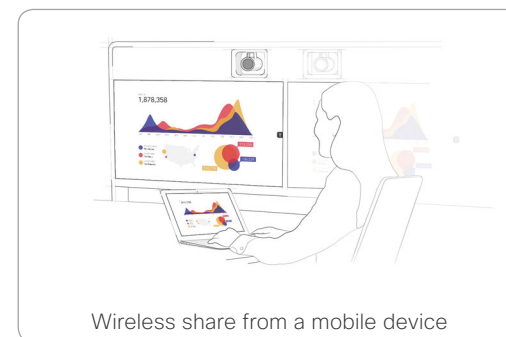
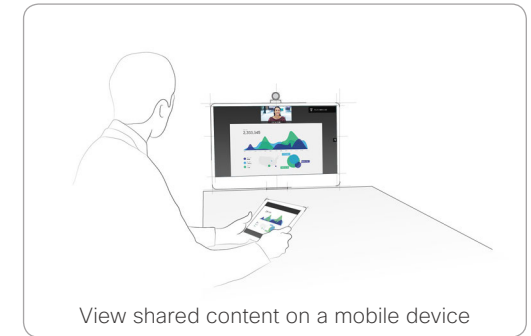
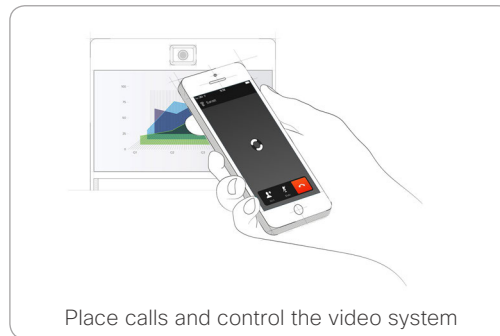
- Dial, mute, adjust volume, hang up
- Available on smartphones and tablets (iOS and Android)

View shared content on a mobile device:

- View shared content, review previous slides, save selected slides
- Available on smartphones and tablets (iOS and Android)

Wireless share from a mobile device:

- Share content without connecting a presentation cable
- Available on laptops (OS X and Windows)



Set up Intelligent Proximity for content sharing (page 2 of 4)

About ultrasound

Cisco video systems emit ultrasound as part of the Proximity feature.

Most people are exposed to ultrasound more or less daily in many environments, including industry, commercial applications and home appliances.

MX Series

In our integrated MX Series systems, the ultrasound sound pressure level is below 75 dB at a distance of 75 cm or more from the loudspeaker.

Even if airborne ultrasound may cause subjective effects for some individuals, it is very unlikely that any effects will occur for levels below 75 dB.

SX Series

For SX Series systems, which use third-party loudspeakers, we do not know the sound pressure level.

The volume control on the remote control or Touch controller does not affect the ultrasound sound pressure level; only the volume control on the loudspeaker itself, and the [Peripherals > Pairing > Ultrasound > Volume > MaxLevel](#) setting has an effect.

Headsets

We do not know the sound pressure level for headsets. Therefore we recommend not to use a headset with MX Series and SX Series video systems, if you have switched **on** Proximity (ultrasound).

Install a Cisco Proximity client

Where to find the clients

You can download the Cisco Proximity clients for smartphones and tablets (Android and iOS), and laptops (Windows and OS X) free of charge from ► <http://proximity.cisco.com>

Clients for smartphones and tablets are also available directly through Google Play (Android) and Apple App Store (iOS).

End-user license agreement

Read the end-user license agreement carefully, ► http://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

Supported operating systems

- iOS 7 and above
 - Android 4.0 and above
 - Mac OS X 10.9 and above
 - Windows 7 and above
- The tile based interface introduced with Windows 8 is not supported.
- The client is launched as a public Beta.

Set up Intelligent Proximity for content sharing (page 3 of 4)

Enable the Proximity services

All Proximity services are **disabled** by default.

1. Sign in to the web interface, and navigate to [Configuration > System Configuration](#).

2. Go to [Proximity > Mode](#), and switch Proximity **On**.

The video system starts sending ultrasound pairing messages.

3. Enable the services you want to allow.

In order to fully utilise the Proximity functionality, we recommend that you enable all services.

Place calls and control the video system:

- Go to [Proximity > Services > CallControl](#) and choose **Enabled**.

View shared content on a mobile device:

- Go to [Proximity > Services > ContentShare > FromClients](#) and choose **Enabled**.

Wireless share from a mobile device:

- Go to [Proximity > Services > ContentShare > ToClients](#) and choose **Enabled**.

Disable Proximity temporarily

You can temporarily disable Proximity in a meeting from the Touch controller.

- Tap the contact information in the upper left corner of the Touch controller, and switch Proximity on or off.

This is useful in meetings where you want to prevent devices in the room from receiving content.

You cannot temporarily disable Proximity if using the TRC6 remote control.

The Proximity indicator

The Proximity indicator is shown on both the main display and the Touch controller.



Proximity is On, and at least one service is enabled.



The Proximity feature is temporarily disabled.

About Proximity

When Proximity is switched **On**, the video system transmits ultrasound pairing messages.

The Proximity feature is switched **Off** by default, because the use of third-party speakers may need additional testing for Proximity to work as expected. In rare cases the ultrasound may cause audio artifacts. If so, consider to decrease the maximum ultrasound volume with the [Peripherals > Pairing > Ultrasound > Volume > MaxLevel](#) setting

The ultrasound pairing messages are received by nearby devices with Proximity clients, and triggers the authentication and authorization of the device.

For the best user experience, Cisco recommends that Proximity always is switched **On***

In order to get full access to Proximity, the Proximity services ([Proximity > Services > ...](#)) must be **Enabled** as well.

* We recommend not to use a headset, if you have switched **on** Proximity (ultrasound).

Set up Intelligent Proximity for content sharing (page 4 of 4)

Room considerations

Room acoustics

- Rooms with hard surfaces may cause challenges due to severe audio reflections. Acoustical treatment of meeting rooms is always highly recommended for the best meeting experience as well as Intelligent Proximity performance.
- Cisco recommends only one video system with Intelligent Proximity enabled in a room. Otherwise, interference is likely to occur, which may lead to problems with device discovery and session maintenance.

Basic troubleshooting

Cannot detect devices with Proximity clients

- Check if the video system is in standby mode. Ultrasound is not transmitted if the speakers (for example a TV in standby mode) are turned off.
- Check the speaker volume. The volume control on a speaker itself (not the volume controlled using the remote control or Touch 10) affects the ultrasound volume. If the volume is too low, the listening devices cannot detect the ultrasound pairing messages.
- Some Windows laptops are not able to record sound in the ultrasound frequency range (20kHz-22 kHz). This can be due to frequency limitations with the soundcard, sound driver or the internal microphone of the particular device. Refer to the Support forum for more information.

Audio artifacts

If you can hear audio artifacts, like humming or clipping noise, decrease the maximum ultrasound volume (*Peripherals > Pairing > Ultrasound > Volume > MaxLevel*).

About privacy

In the Cisco Privacy statement and the Cisco Proximity Supplement you find information about data collection in the clients and privacy concerns that needs to be considered when deploying this feature in the organisation. Refer to:
▶ <http://www.cisco.com/web/siteassets/legal/privacy.html>

You can temporarily disable Proximity in a meeting from the Touch controller. This is useful in meetings where you want to prevent devices in the room from receiving content.

You cannot temporarily disable Proximity if using the TRC6 remote control.

Additional resources

Cisco Intelligent Proximity site:
▶ <https://www.cisco.com/go/proximity>
Support forum:
▶ <https://www.cisco.com/go/proximity-support>

Adjust the video quality to call rate ratio

Optimal definition profile

The optimal definition profile should reflect the lighting conditions in the video conferencing room and the quality of the camera (video input source). The better the lighting conditions and the better the quality of the camera, the higher the profile should be used. In good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate.

Generally, the Medium profile is recommended. However, if the lighting conditions are very good, we recommend that you test the endpoint on the various Optimal Definition Profile settings before deciding on a profile. The High profile may be set in order to increase the resolution for a given call rate.

Some typical resolutions used for different optimal definition profiles, call rates and transmit frame rates are shown in the table. The resolution and frame rate must be supported by both the calling and called systems.

Threshold for sending video at 60 fps

Use the *Video Input Connector n OptimalDefinition Threshold60fps* setting to decide when to allow sending video at 60 fps.

For all resolutions lower than this threshold, the maximum transmitted frame rate will be 30 fps; for higher resolutions, 60 fps is possible if the available bandwidth is adequate.

Video input quality settings

The *Video Input Connector n Quality* setting must be set to **Motion** for the optimal definition settings to take any effect. With the video input quality set to **Sharpness**, the endpoint will transmit the highest resolution possible, regardless of frame rate.

Sign in to the web interface and navigate to [Configuration > System Configuration](#).

1. Go to [Video > Input > Connector n > Quality](#) and set the video quality parameter to **Motion**.
2. Go to [Video > Input > Connector n > OptimalDefinition > Profile](#) and choose the preferred optimal definition profile.
3. Go to [Video > Input > Connector n > OptimalDefinition > Threshold60fps](#) to set the threshold below which the maximum transmitted frame rate will be 30 fps.

Typical resolutions used for different optimal definition profiles, call rates and frame rates								
	Frame rate	Optimal Definition Profile	Call rate					
			768 kbps	1152 kbps	1472 kbps	2560 kbps	4 Mbps*	6 Mbps*
H.265 (only in SIP calls)	30 fps	Normal	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		Medium	1280×720	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080
		High	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080
	60 fps	Normal	768×448	1024×576	1280×720	1280×720	1280×720	1280×720
		Medium	1024×576	1280×720	1280×720	1280×720	1280×720	1280×720
		High	1280×720	1280×720	1280×720	1280×720	1280×720	1280×720
H.264	30 fps	Normal	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		Medium	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		High	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
	60 fps	Normal	640×360	768×448	1024×576	1280×720	1280×720	1920×1080
		Medium	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
		High	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

* H.265 is preferred over H.264, and the maximum bit rate for H.265 is 3 Mbps. When the user sets a higher bit rate, the codec will still use H.265 at 3 Mbps as long as all codecs involved supports H.265.

Packet loss resilience – ClearPath

ClearPath introduces several mechanisms for advanced packet loss resilience. These mechanisms increase the experienced quality when you use your video system in an error prone environment.

ClearPath is a Cisco proprietary protocol. All endpoints running CE software support ClearPath.

If the involved endpoints and infrastructure elements support ClearPath, all packet loss resilience mechanisms are used in point-to-point connections (including hosted conferences). Only some of the mechanisms are supported in MultiSite conferences.

Use a custom wallpaper

Sign in to the web interface, and navigate to [Configuration > Personalization](#).

Activate or deactivate the custom wallpaper

If a custom wallpaper is stored on the video system, it will be shown here.

Click [None](#) to deactivate the wallpaper; click [Custom](#) to activate it. The chosen option is highlighted.

Upload a custom wallpaper

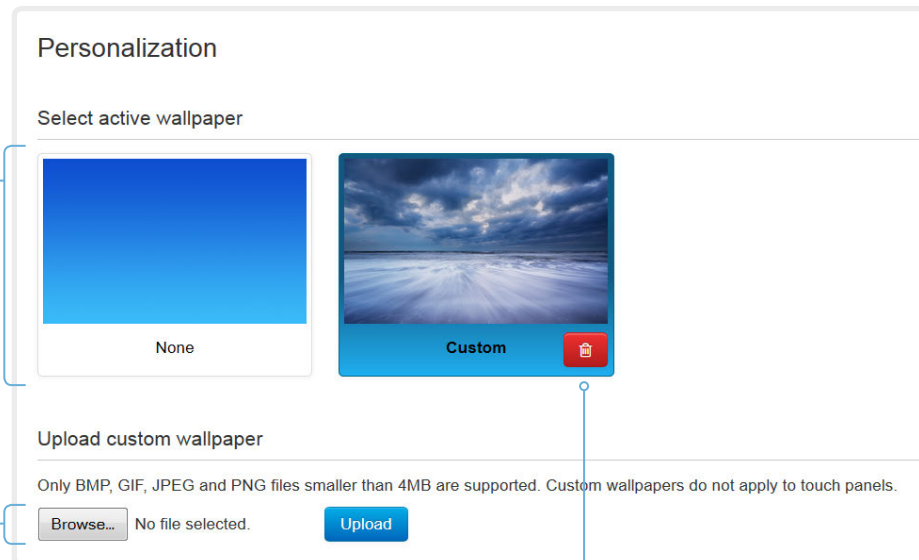
An existing wallpaper will be overwritten.

1. Click [Browse...](#) and locate the custom wallpaper image file.
2. Click [Upload](#) to save the file on the video system.

Supported file formats: BMP, GIF, JPEG, PNG

Maximum file size: 4 MByte

The custom wallpaper is automatically activated once uploaded.



Delete the custom wallpaper

[Delete](#) fully removes the custom wallpaper from the video system.

You have to upload it anew if you want to start using it again.

About wallpapers

If you want the company logo or another custom picture as background on the main display, you may upload and use a *custom wallpaper*.

Only one custom wallpaper can be stored on the video system at a time; a new custom wallpaper overwrites an existing one.

When you use a custom wallpaper, these items are removed from the main display:

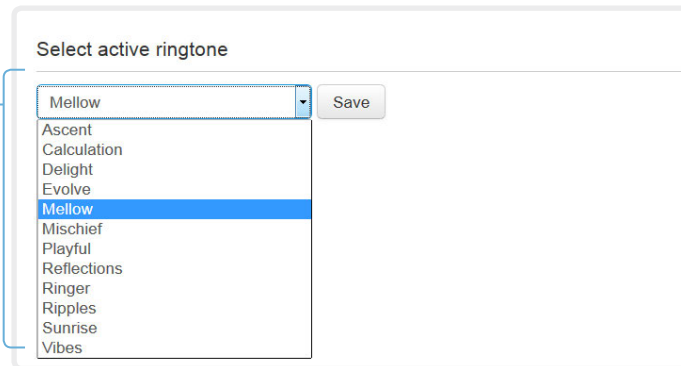
- The clock
- The list of upcoming meetings

Choose ringtone

Sign in to the web interface, and navigate to [Configuration > Personalization](#).

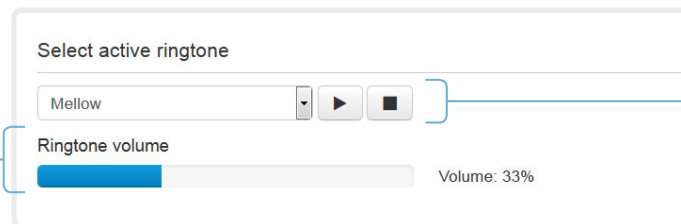
Change the ringtone

1. Choose a ringtone from the drop-down list.
2. Click [Save](#) to make it the active ringtone.



Set the ringtone volume

Use the slide bar to adjust the ringtone volume.



Play back the ringtone

Click the play button (▶) to play back the ringtone.

Use the stop button (■) to end the playback.

About ringtones

A set of ringtones are installed on the video system. You should use the web interface to choose a ringtone, and set the ringtone volume.

You can play back the chosen ringtone from the web interface. Note that the ringtone will be played back on the video system itself, and not on the computer running the web interface.

Manage local contacts

Sign in to the web interface and navigate to [Configuration > Local Contacts Management](#).

Import/Export contacts from file

Click [Export](#) to save the local contacts in a file; and click [Import](#) to bring in contacts from a file.

Note that all current local contacts are discarded when you import new contacts from a file.

Add or edit a contact

1. Click [Add contact](#) to make a new local contact, or click a contacts name followed by [Edit contact](#).

2. Fill in or update the form that pops up.

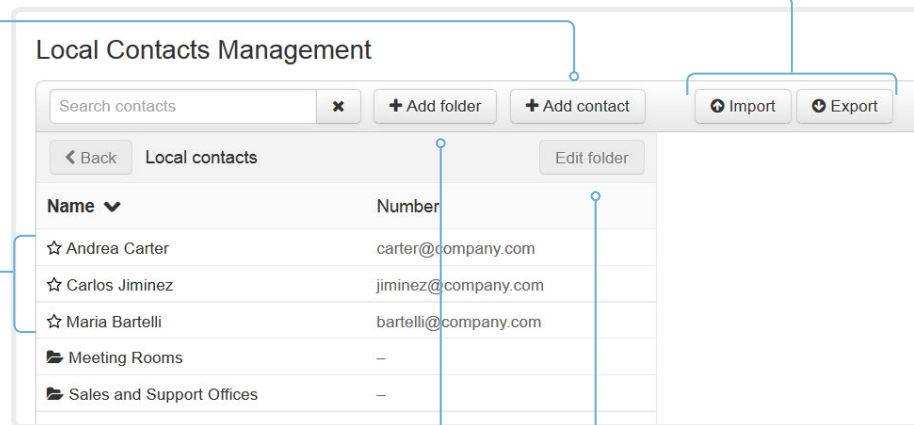
Choose a folder in the folder drop down list in order to store the contact in a sub-folder.

Click [Add contact method](#) and fill in the new input fields if you want to store more than one contact method for the contact (for example video address, telephone and mobile number).

3. Click [Save](#) to store the local contact.

Delete a contact

1. Click a contacts name followed by [Edit contact](#).
2. Click [Delete](#) to remove the local contact.



Add or edit a sub-folder

1. Click [Add folder](#) to make a new sub-folder, or click one of the listed sub-folders followed by [Edit folder](#) to change an existing sub-folder.
2. Fill in or update the form that pops up.
3. Click [Save](#) to create or update the folder.

Delete a sub-folder

1. Click [Edit folder](#).
2. Click [Delete](#) to remove the folder and all its contacts and sub-folders. Confirm your choice in the dialog that pops up.

Where to find the local contacts

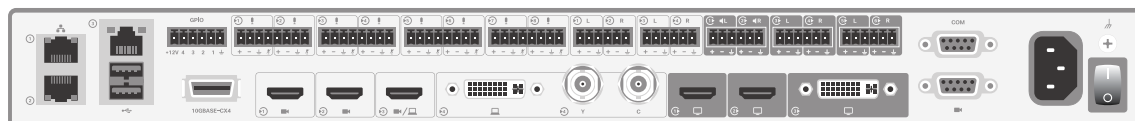
Touch controller: Tap [Contacts > Favorites](#) to find all local contacts.

Web interface: Click [Call Control](#), and open the [Local](#) tab in the [Contacts](#) section.


Chapter 3

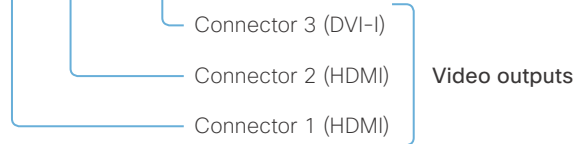
Peripherals

Connect monitors (page 1 of 2)



You can connect up to three monitors to the codec. The codec distributes the layout on all available monitors.

 Always switch off power when you connect and disconnect monitors and other peripherals.



Automatic setup

There is no special configuration needed on the codec in order to support dual monitors or triple monitors scenarios. By default the number of monitors are auto-detected, and the role of each monitor - whether it is intended to be the first, second, or third monitor - is automatically set according to the physical connections.

For example, if the total number of monitors are three, the following settings will be assumed when set to **Auto**:

- [Video > Monitors](#) : **Triple**
- [Video > Output > Connector 1 > MonitorRole](#) : **First**
- [Video > Output > Connector 2 > MonitorRole](#) : **Second**
- [Video > Output > Connector 3 > MonitorRole](#) : **Third**

These settings can be changed if necessary, but for ease of use no configuration is required in order to use the default values.

When do you need manual setup

You can override the default behavior by setting one or more settings manually. You need manual setup when you want to:

- Dedicate a monitor to only show presentations
- Use one of the outputs for a recorder
- Replicate the same layout on more than one monitor
- Show the on-screen messages and indicators (OSD) on another monitor than the video output with the lowest number
- Set the resolution manually, e.g. if the codec fails to detect the native resolution and refresh rate of a monitor

About video outputs

SX80 has two HDMI video outputs and one DVI-I output. All outputs can be used simultaneously.

Typically, the outputs are used for monitors or other displays. You can also connect a recorder.

As default, there is audio on only one of the HDMI outputs: audio is switched **On** on Connector 1, and **Off** on Connector 2.

If you want audio on Connector 2, refer to the CE Console application that is introduced in the [Advanced customization of audio and GPIO](#) appendix.

Connect monitors (page 2 of 2)

Manual setup

The automatic setup works well for common single monitor, dual monitors, and triple monitors scenarios. For more complex scenarios, you may need manual configuration.

Sign in to the web interface and navigate to [Configuration > System Configuration](#), to find the settings referred below.

Set a role for each monitor

Define a role for each monitor with the [Video > Output > Connector n > MonitorRole](#) setting.

Choose monitor roles that match your monitor setup.

Set the number of monitors

Set the number of monitors with different layouts in your setup with the [Video > Monitors](#) setting.

When set to **Auto**, the codec automatically detects if a monitor is connected to a connector, and thereby also determines the number of monitors in the setup.

The other options allow you to fix a single, dual, or triple monitor setup; and to dedicate one monitor for presentations.

Choose on which monitor to display messages and indicators

Define on which monitor to display the messages and indicators on-screen with the [UserInterface > OSD > Output](#) setting.

When set to **Auto**, the codec determines which monitor to use based on the number of the connector.

Set the monitor resolution and refresh rate

The codec reads the native resolution of a monitor and outputs this if possible. Typically, this gives the best possible picture for the monitor.

If auto-detection of resolution and refresh rate fails, you must set the resolution manually with the [Video > Output > Connector n > Resolution](#) setting.

About the number of monitors and the role of each monitor

The [Video > Output > Connector n > MonitorRole](#) setting assigns a role to the monitor that is connected to the output. The monitor role decides which layout (call participants and presentation) will appear on the monitor.

Monitors with the same monitor role get the same layout; monitors with different monitor roles have different layouts.

The [Video > Monitors](#) setting must reflect *the number of different layouts* in your room setup.

Most often the number of different layouts are the same as the number of physical monitors, but not always; if exactly the same layout shall be repeated on two or more monitors, the number of different layouts are less.

Note that a monitor can be reserved for presentations.

Example 1:

Three monitors in total, and the third monitor is dedicated to only show presentations:

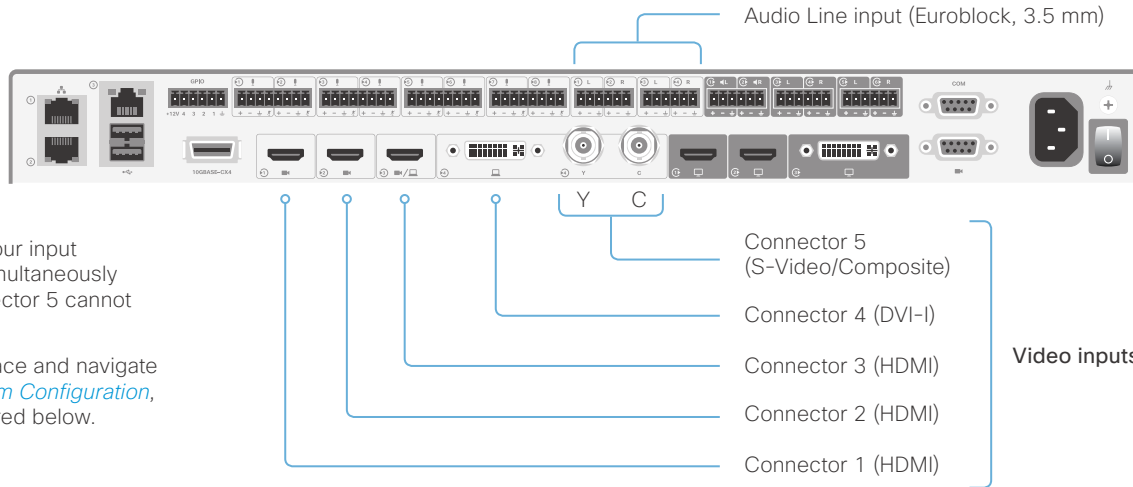
- [Video > Monitors](#) : **TriplePresentationOnly**
- [Video > Output > Connector 1 > MonitorRole](#) : **Auto**
- [Video > Output > Connector 2 > MonitorRole](#) : **Auto**
- [Video > Output > Connector 3 > MonitorRole](#) : **Auto**
- [UserInterface > OSD > Output](#) : **Auto**

Example 2:

Two monitors in total, and a recording device is attached to Connector 3 (DVI). OSD on the monitor on Connector 2:

- [Video > Monitors](#) : **Auto**
- [Video > Output > Connector 1 > MonitorRole](#) : **Auto**
- [Video > Output > Connector 2 > MonitorRole](#) : **Auto**
- [Video > Output > Connector 3 > MonitorRole](#) : **Recorder**
- [UserInterface > OSD > Output](#) : **2**

Connect input sources (page 1 of 2)



You can connect up to four input sources to the codec simultaneously (Connector 4 and Connector 5 cannot be used simultaneously).

Sign in to the web interface and navigate to [Configuration > System Configuration](#), to find the settings referred below.

Connect a camera

The codec supports maximum three cameras. Typically, cameras are connected to the HDMI inputs.

Always use Connector 1 (HDMI) for the main camera.

If you have a Cisco TelePresence SpeakerTrack 60 camera assembly, connect its two cameras to Connector 1 (HDMI) and Connector 2 (HDMI).

Refer to the SX80 installation guide or the camera documentation how to connect a camera to power, Ethernet and/or camera control.

Connect a computer

Connect a computer to a video input in order to share content locally or with conference participants. The codec supports two computers simultaneously.

Typically, computers are connected to Connector 3 (HDMI) or Connector 4 (DVI-I).

To get audio when using DVI-I, you must also connect the computer to one of the codec's *Audio Line* inputs (Euroblock).

Audio Line input (Euroblock, 3.5 mm)

Connector 5 (S-Video/Composite)

Connector 4 (DVI-I)

Connector 3 (HDMI)

Connector 2 (HDMI)

Connector 1 (HDMI)

Video inputs

About video inputs

SX80 has three HDMI video inputs, one DVI-I input, and one combined S-Video/Composite video input.

Typically, the inputs are used for cameras and computers. You can also connect other types of video and content sources.

The DVI-I and combined S-Video/Composite video inputs cannot be used simultaneously.

Connect input sources (page 2 of 2)

About video and content quality

Use the [Video > Input > Connector n > Quality](#) setting to optimize quality with respect to motion or sharpness.

Typically, you should choose **Motion** when a large number of participants are present or when there is a lot of motion in the picture. Choose **Sharpness** when you want the highest quality of detailed images and graphics.

The default value is **Motion** for Connector 1, 2 and 5; and **Sharpness** for Connector 3 and 4.

Set type and name for the input sources

We recommend that you set type and name for the input sources:

- [Video > Input > Connector n > InputSourceType](#)
- [Video > Input > Connector n > Name](#)

These settings determine the names and icons that are shown on the user interfaces. Intuitive names and icons make source selection easier.

Set up speaker tracking

Sign in to the web interface and navigate to [Configuration > System Configuration](#), to find the settings referred.

Use the [Cameras > SpeakerTrack > Mode](#) setting to enable or disable speaker tracking.

Off: Speaker tracking is switched off permanently.

Auto: Speaker tracking is enabled in general. Users can switch it on or off instantly with the camera control panel on the Touch controller.

Tracking mode

The tracking mode defines how fast the camera view switch to a new speaker when the tracking algorithm detects a change.

Use the [Cameras > SpeakerTrack > TrackingMode](#) setting to select between the two modes.

Auto: This is the default setting.

Conservative: The system reacts slower to detected changes, and the camera view will switch to a new speaker later.

You can also use the Administrator Settings menu on the Touch controller to switch between the two tracking modes.

- Tap [Settings > Administrator](#) and sign in.
- Tap [Tracking](#), and set [Tracking Mode](#) to **FAST** (auto) or **NORMAL** (conservative).

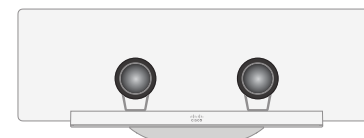
About speaker tracking

The following Cisco TelePresence products support speaker tracking:

- MX700 and MX800 with dual camera



- SpeakerTrack 60 camera



The two cameras in the assembly work together with a built-in microphone array to automatically track and show the person that speaks.

Set up the Snap to Whiteboard feature (page 1 of 3)

The Snap to Whiteboard feature extends the speaker tracking functionality.

A speaker track camera tracks the person talking automatically, and normally the camera moves to cover the talking person only. With the Snap to Whiteboard extension enabled, the camera also covers the whiteboard when the person talking stands next to it.

A system administrator must define the whiteboard position using the wizard on the Touch controller.

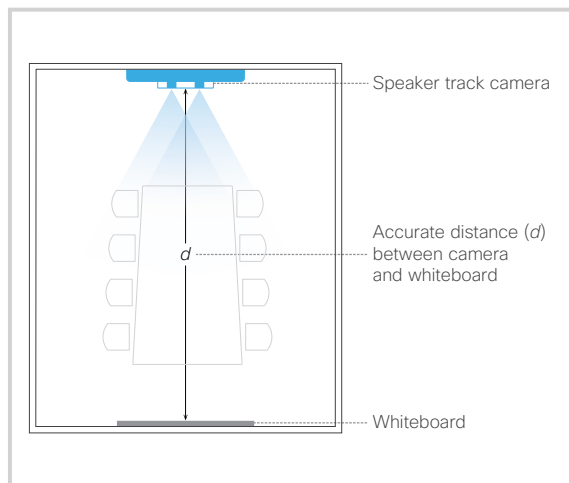
Prerequisites

- Camera that supports speaker tracking
 - MX700 and MX800 with dual camera, or
 - SX80 with SpeakerTrack 60 camera
- *Cameras > SpeakerTrack > Mode* set to **Auto**

Since Snap to Whiteboard is an extension to speaker tracking, tracking must be switched on when using Snap to Whiteboard.



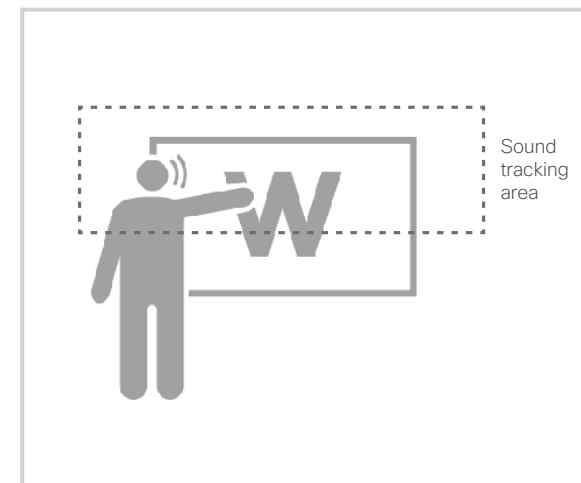
Preparations



Whiteboard position

The whiteboard must be placed across the room from the camera, as shown in the illustration.

When configuring the feature, you need to know the accurate distance between the camera and the whiteboard.



Speaker position

The *Sound tracking area* is from half the whiteboard and up.

Thus, the person presenting on the whiteboard must stand upright next to the whiteboard. He or she cannot move about in the room.

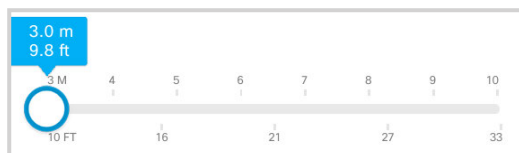
Set up the Snap to Whiteboard feature (page 2 of 3)

Define the whiteboard area

Use the wizard on the Touch controller to define the whiteboard area.

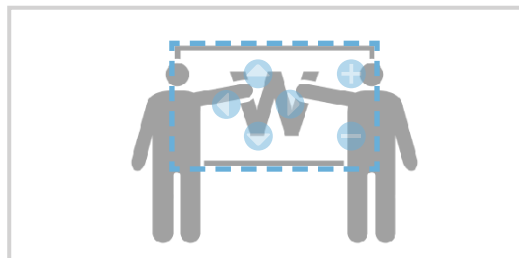
1. Tap the contact information in the upper left corner of the Touch controller and open the *Settings* menu.
2. Tap *Administrator*, and sign in with administrator credentials.
3. Tap *Tracking*.
4. Tap *Configure Snap to Whiteboard* or *Reconfigure Snap to Whiteboard* (depends whether you configure the feature for the first time or not) to start the wizard.

5. Follow the instructions in the wizard - use the back button, if you want to redo a step:
 - Set the distance between the camera and the whiteboard. Slide the circle to the correct distance on the ruler.



It is important that the distance is measured accurately.

- Position the camera (pan, tilt, zoom) to frame the whiteboard as accurate as possible.



- Fine tune the position (pan, tilt, zoom) of both cameras so that they show the same image.
- Stand by the whiteboard and start talking.

If the feature is correctly configured, the camera will move to a position that covers both the whiteboard and the person that is talking.

Troubleshooting

If the camera does not move to the whiteboard position when the person who is talking stands next to the whiteboard, check the following and redo the required steps in the wizard:

- Check that the whiteboard is placed across the room from the camera.
- Check that the distance between the camera and whiteboard is measured accurately.
- The person who is talking must be close to the whiteboard. Furthermore the person must stand upright, so that the sound comes from the upper half of the whiteboard area.

Set up the Snap to Whiteboard feature (page 3 of 3)

Switch the Snap to Whiteboard feature on or off

1. Tap the contact information in the upper left corner of the Touch controller and open the [Settings](#) menu.
2. Tap [Administrator](#), and sign in with administrator credentials.
3. Tap [Tracking](#).
4. When *Snap to Whiteboard* is set to **ON** the camera will capture both the person and the whiteboard when the person that talks is close to the whiteboard.

Choose **OFF** if you want only the person to be captured.

Alternatively, use the [Cameras > SpeakerTrack > Whiteboard > Mode](#) setting on the web interface to switch the Snap to Whiteboard feature On or Off.



Since Snap to Whiteboard is an extension to speaker tracking, tracking must be switched on when using Snap to Whiteboard.



Briefing room set-up (page 1 of 3)

The briefing room set-up is designed to provide easy set up, management and use of a room for education, training or similar.

The set-up is tailored around the following room modes:

- *Local Presenter* (the presenter is in the room)
- *Remote Presenter* (the presenter is calling in)
- *Discussions* (for discussions between different sites with local presenter in the room)

The briefing room is available as a room type template, which means that the required configurations are pushed automatically to the codec when you select the template.

In order for these configurations to match the room, it is important that the room is set up correctly, and that cameras and displays are connected exactly as specified in this chapter.

Required equipment

- Codec: SX80 codec with Touch 10.
- Three displays: They are referred to as Presentation display, Remote presenter display, and Remote audience display (see blue print to the right).
- Two cameras: They are referred to as Audience camera, and Presenter camera (see blue print to the right). We recommend the Cisco TelePresence SpeakerTrack 60 camera assembly as Audience camera, but a single camera can also be used. We recommend Cisco TelePresence Precision 60 as Presenter camera.
- Microphones: We recommend the Cisco TelePresence Ceiling Microphone for good coverage of the room. Other microphone solutions can also be used.
- Speakers: We recommend good quality stereo speakers placed next to the Presentation and Remote presenter displays.



Briefing room set-up



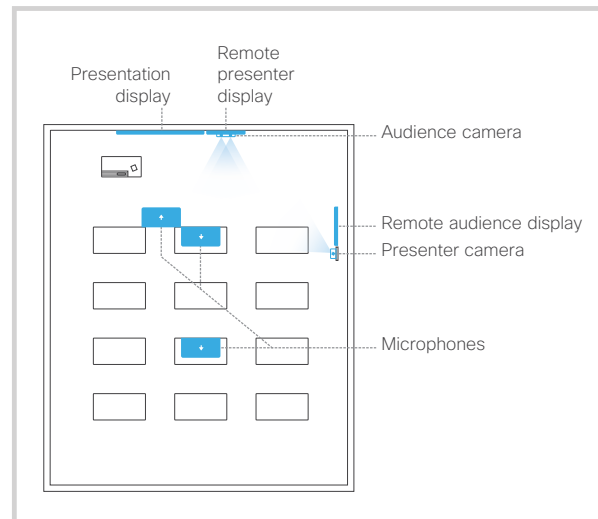
Local Presenter



Remote Presenter




Discussions

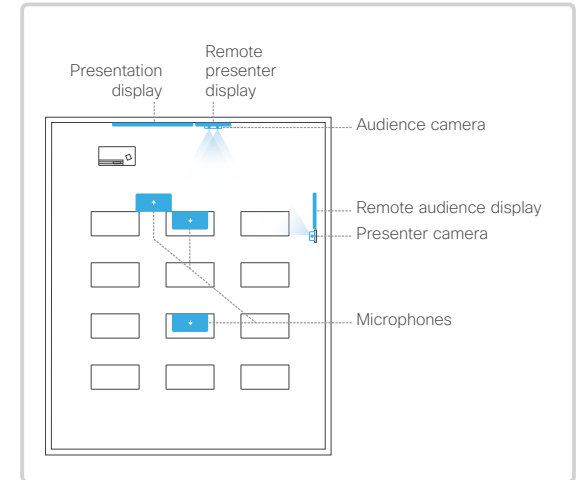
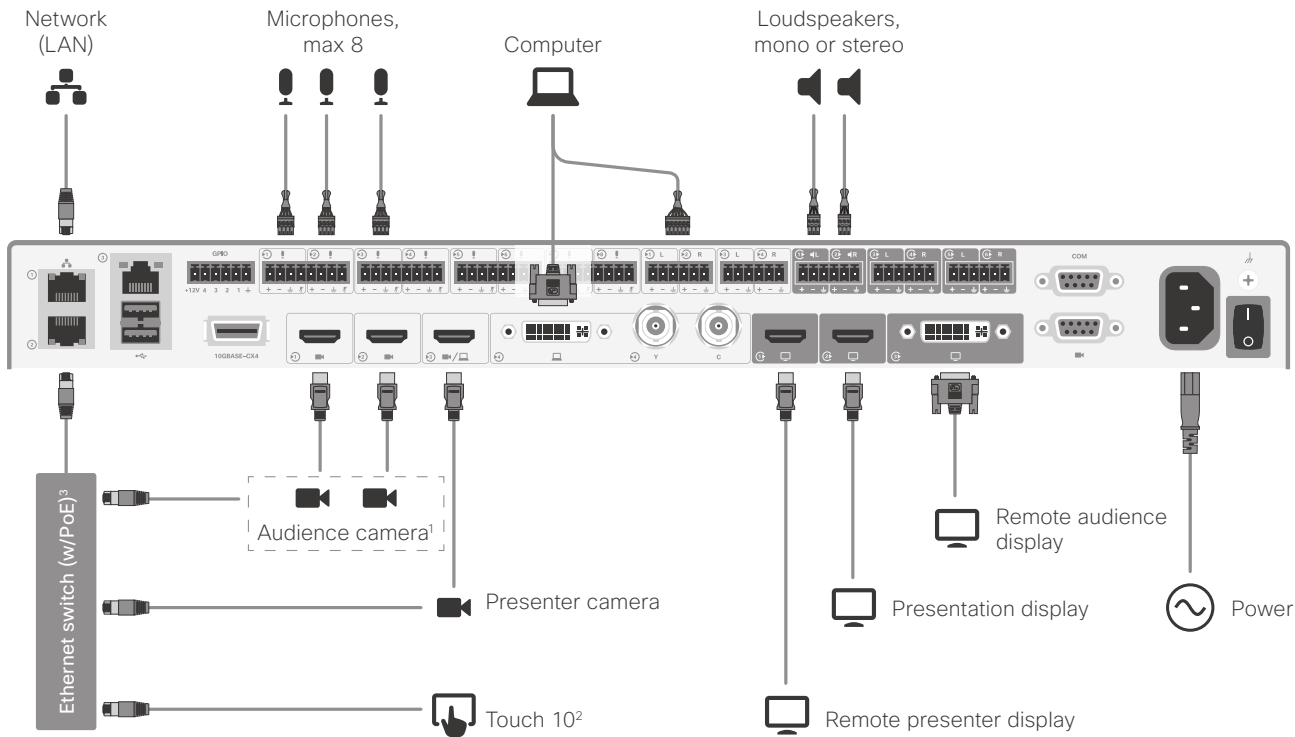


Briefing room blue print

Briefing room set-up (page 2 of 3)

Connecting cables

 It is very important to connect the cameras and monitors to the codec as illustrated; otherwise the configuration that is pushed to the codec when selecting the *Briefing* room type template will not match your actual set-up.



¹ If the Audience camera unit is a single camera, you should use camera input 1 for the Audience camera and camera input 3 for the Presenter camera.

² If the Ethernet switch does not provide Power over Ethernet (PoE), you need a mid-span PoE injector for Touch 10. Refer to the [Connect the Touch 10 controller](#) chapter for more information.

³ The Ethernet switch may be connected to either Network port 2 as illustrated, or to Network port 3. It cannot be connected to Network port 1, which is reserved for the LAN connection.

Briefing room set-up (page 3 of 3)

Configure the codec

1. Sign in to the web interface, and navigate to [Configuration > Room Types](#).
2. Click the [Briefing](#) thumbnail to push the corresponding configuration to the codec.

Note that the cameras and displays must be connected as described in the [▶ Connecting cables](#) chapter.

Change room mode while in a conference

These are the pre-defined modes for the Briefing room:

- *Local Presenter* (the presenter is in the room)
- *Remote Presenter* (the presenter is calling in)
- *Discussions* (for discussions between different sites with local presenter in the room)

Switching from one mode to another implies changing the camera input sources and changing the remote and local screen layouts.

Switch to another room mode manually

While in a conference, you can switch to another mode using the Touch controller.

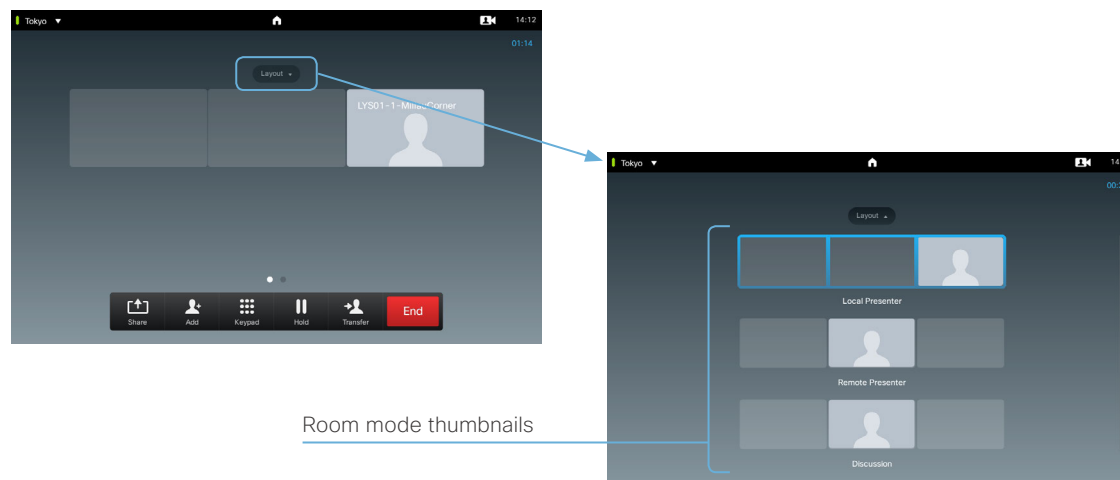
1. Tap [Layout](#) on the Touch controller.
2. Tap the thumbnail that represents the mode you want to change to.

Switch room modes automatically

The following situations cause an automatic mode change:

- When you start to share a presentation locally, the system will automatically change to the *Local Presenter* mode.
- When the far end starts to share a presentation, the system will automatically change to the *Remote Presenter* mode.

Note the following exception: The room mode will not change automatically if the current mode is *Discussions*.



Real-time communication requirements for displays

We have put in a lot of effort to minimize the camera to screen delay on our TelePresence endpoints, and also to detect and compensate for total delay between the audio and video components.

We recommend that you use displays with low delay to increase the naturalness of communications. We also recommend that you test a sample before ordering a large number of displays.

Delay through most displays is often very high (>100 ms) and is therefore detrimental to real-time communication quality.

The following display settings may reduce the delay:

- Activate “Game” mode, “PC” mode or similar modes that are designed to reduce the response time and normally also the delay
- Deactivate motion smoothing, like “Motion Flow”, “Natural Motion”, or any other video processing that introduces additional delay
- Deactivate advanced audio processing, like “Virtual Surround” effects and “Dynamic Compression”, which will make any acoustic echo canceller malfunction
- Change to a different HDMI input

Connect the Touch 10 controller (page 1 of 3)

In order to use Touch 10 as user interface for SX80, Touch 10 must either be directly connected to the codec as described on this page, or paired to the codec via the network (LAN) as described on the next page. The latter is referred to as remote pairing.

Connect Touch 10 directly to the codec

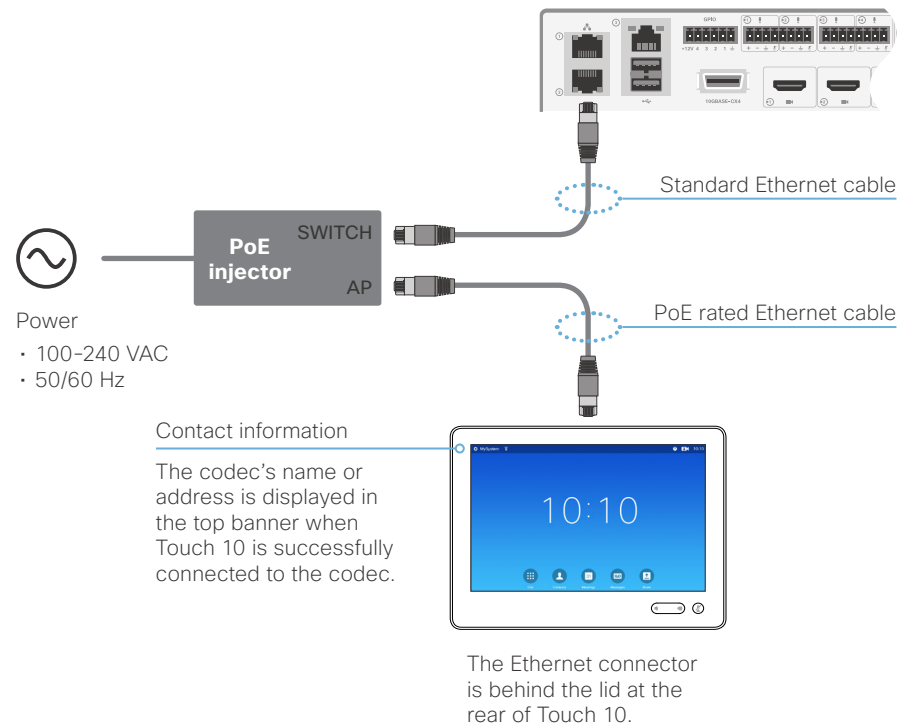
Connect Touch 10 to the codec's 2nd or 3rd Ethernet connector as illustrated.

Note that SX80 does not provide Power over Ethernet (PoE), so you need a mid-span PoE injector to power Touch 10.

Touch 10 set-up

Once Touch 10 is connected to power, the set-up procedure begins. Follow the instructions on screen.

If Touch 10 needs software upgrade, new software will be downloaded from the codec and installed on the unit automatically as part of the set-up procedure. Touch 10 restarts after the upgrade.



About the SX80 network ports

SX80 has three network ports. Network port 1 is reserved for the connection to LAN, while Network ports 2 and 3 should be used for peripherals like cameras and Touch 10.

If you have more than two peripheral units requiring an Ethernet connection, you can insert an Ethernet switch between Network port 2 or 3 and the peripherals.

Connect the Touch 10 controller (page 2 of 3)

Connect Touch 10 to the codec via the network (LAN)

Connect Touch 10 and the codec to network wall sockets or to a network switch as illustrated.

Touch 10 set-up

Once Touch 10 is connected to power, the set-up procedure begins. Follow the instructions on screen.

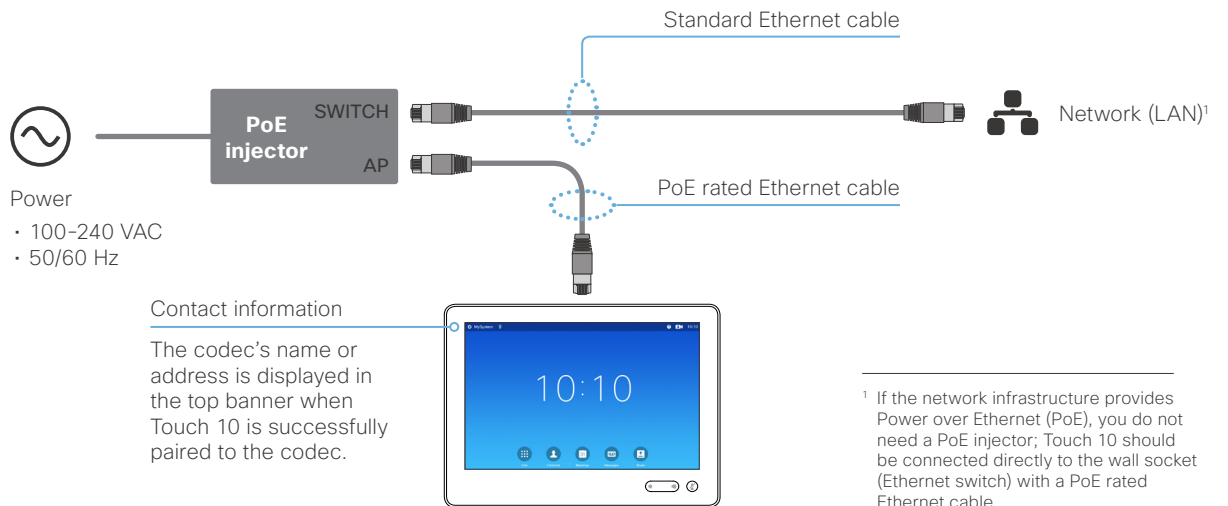
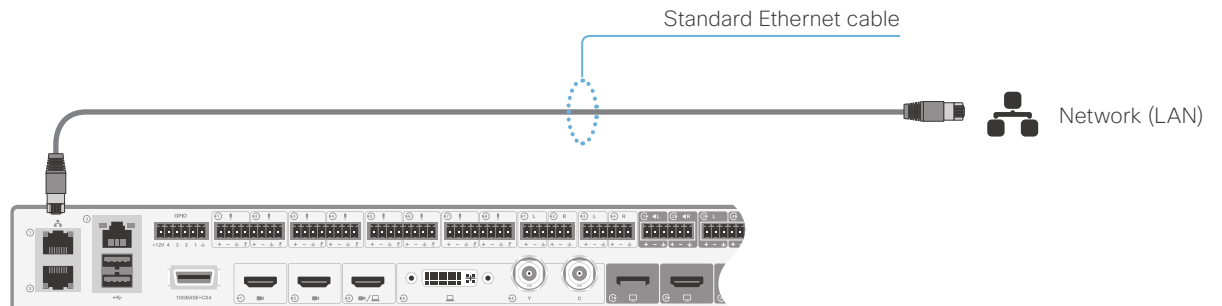
When the *Select codec to pair with* dialog appears, note the following:

- A list of codecs signalling that they are available for pairing will show up in the dialog. Tap the name of the codec you want to pair to followed by *Start Pairing*.

Note that the following must be fulfilled for a codec to show up in the list:

- The codec and Touch 10 must be on the same subnet.
- The codec must have been restarted within the last 10 minutes. If the codec does not appear in the list, try restarting it.
- If the codec does not appear in the list of available codecs, you can pair the devices manually. Click *Select codec manually...*, enter the IP address or host name of the codec, and tap *Start Pairing*.
- You have to enter the codec's administrator username and password for the pairing process to commence.

If Touch 10 needs software upgrade, new software will be downloaded from the codec and installed on the unit automatically as part of the set-up procedure. Touch 10 restarts after the upgrade.



Contact information
The codec's name or address is displayed in the top banner when Touch 10 is successfully paired to the codec.

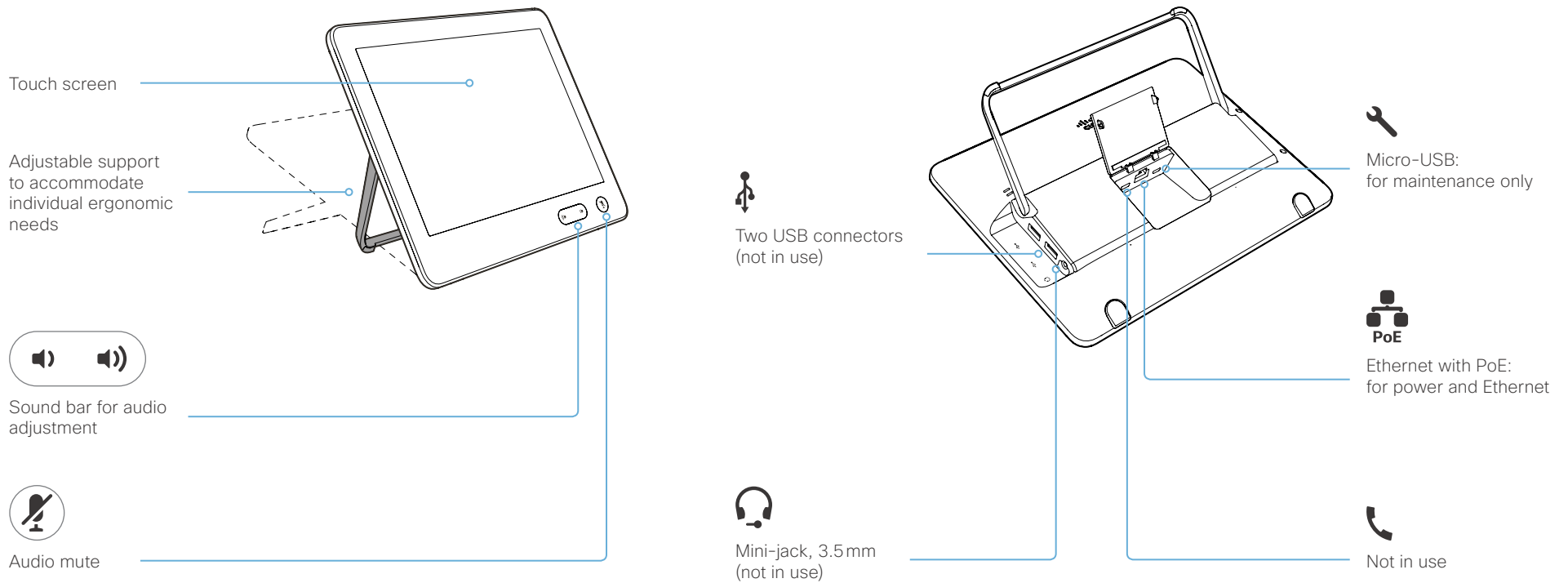
The Ethernet connector is behind the lid at the rear of Touch 10.

¹ If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

For safety, the PoE source must be in the same building as Touch 10. The PoE rated Ethernet cable can be up to 100m (330ft).

Connect the Touch 10 controller (page 3 of 3)

Touch 10 physical interface





Chapter 4

Maintenance

Upgrade the system software (page 1 of 2)

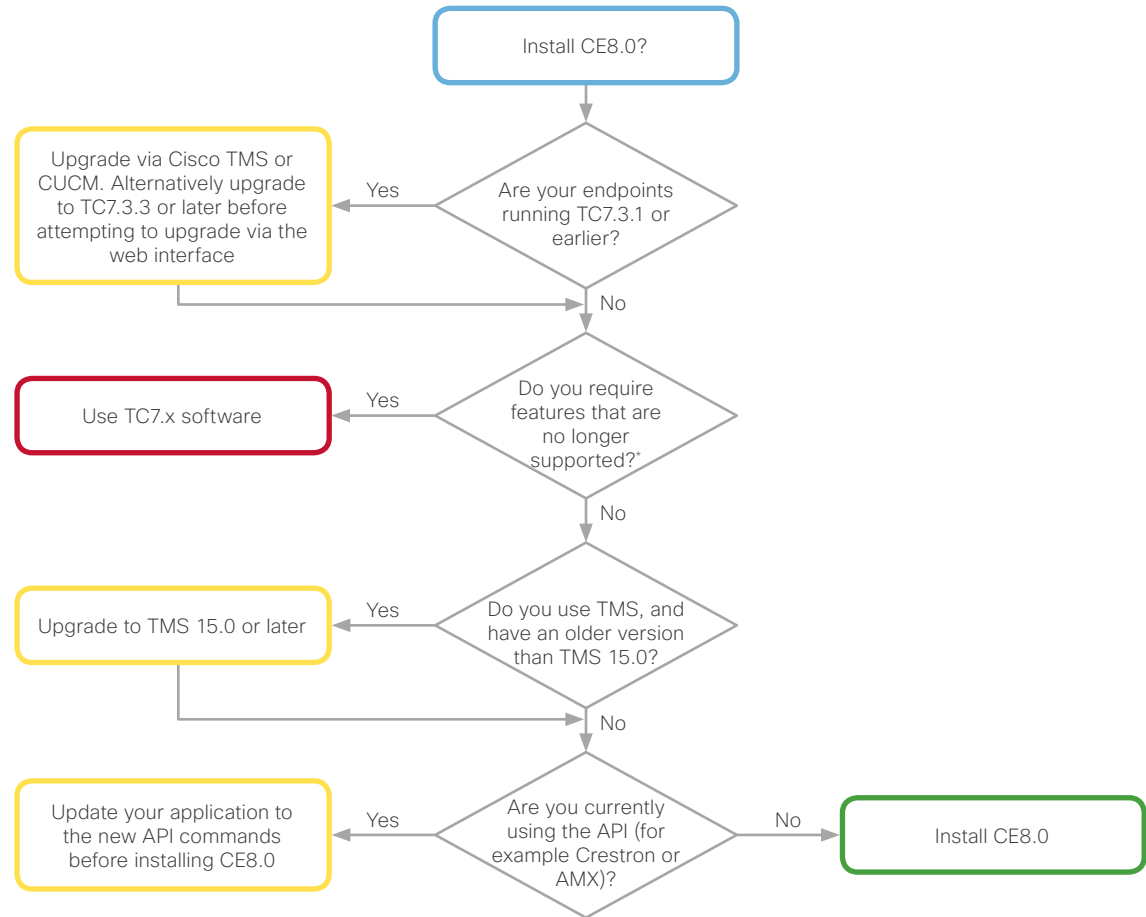
About upgrading from TC to CE software

CE8.0 is the evolution of TC7.x software. CE8.0 inherits years of development in the TC software while being more streamlined, providing higher quality and higher feature velocity.

It is important to carefully consider the upgrade requirements of CE8.0 and the functionality changes compared to TC7.x software before upgrading.

We highly recommend upgrading endpoints to TC7.3.3 or later before proceeding with the upgrade to CE8.0. Upgrading to CE software from TC7.3.0 and TC7.3.1 is not supported via the web interface.

If you do not take into account these considerations, upgrading to CE8.0 can leave you with a non-functioning deployment that requires you to downgrade.



* CE software does not support the following features and products:

- MultiWay conferencing
- CTMS conferencing
- MediaNet
- Displays that do not support 16:9 or 16:10 resolution
- Custom video layouts, video composition using TC Console (temporarily removed). CE Console is for audio and GPIO only

Also note that CE software does not support the EX Series, C Series, Profile Series, and first-generation MX200 and MX300

Upgrade the system software (page 2 of 2)

Sign in to the web interface and navigate to [Maintenance > Software Upgrade](#).

Download new software

For software download, go to the Cisco Download Software web page:

► <http://www.cisco.com/cisco/software/navigator.html>. Then navigate to your product.

The format of the file name is "s52020ce8_0_x.pkg". Each software version has a unique file name.

Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (CE8).

Go to: ► <http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-quick-set-series/tsd-products-support-series-home.html>

About software versions

This video conference system is using CE software. The version described in this document is CE8.0.x.

Install new software

Download the appropriate software package and store it on your computer. This is a .pkg file.

1. Click [Browse...](#) and find the .pkg file that contains the new software.

The software version will be detected and shown.

2. Click [Install software](#) to start the installation process.

The complete installation normally take no longer than 15 minutes. You can follow the progress on the web page. The video system restarts automatically after the installation.

You must sign in anew in order to continue working with the web interface after the restart.

The screenshot shows a web interface titled "Install new software". It contains the following elements:

- A "Software" label followed by a "Browse..." button and the text "No file selected."
- A "Detected version" label followed by the text "Please select a file"
- A blue "Install software" button at the bottom.

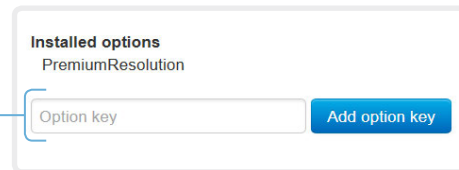
Add option keys

Sign in to the web interface and navigate to [Maintenance > Option Keys](#).

Add an option key

1. Enter an *Option Key* in the appropriate text input field.
2. Click [Add option key](#).

If you want to add more than one option key, repeat these steps for all keys.



The screenshot shows a web interface section titled "Installed options". Underneath, the text "PremiumResolution" is displayed. Below this, there is a text input field with the placeholder text "Option key" and a blue button labeled "Add option key". A blue line from the text "Option key" in the first step of the instructions points to the input field.

About option keys

Your video system may or may not have one or more software options installed. In order to activate the optional functionality the corresponding *option key* must be present on the video system.

Each video system has unique option keys.

Option keys are not deleted when performing a software upgrade or factory reset, so they need to be added only once.

Contact your Cisco representative to obtain information about available options, and how to get the required key(s).

System status

System information overview

Sign in to the web interface to see the *System Information* page.

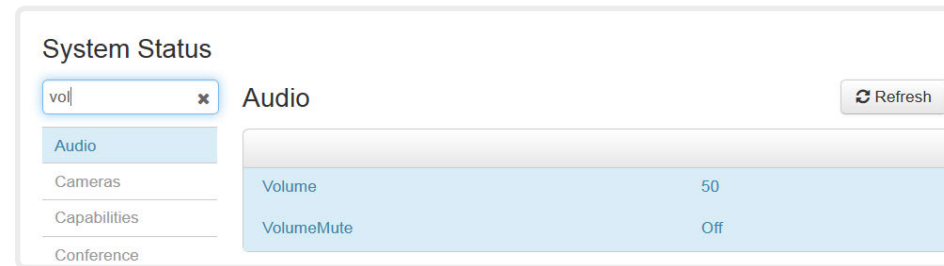
This page shows the product type, system name and basic information about the hardware, software, installed options and network address. Registration status for the video networks (SIP and H.323) is included, as well as the number/URI to use when making a call to the system.

Detailed system status

Sign in to the web interface, and navigate to [Configuration > System Status](#) in order to find more detailed status information*.

Search for a status entry

Enter as many letters as needed in the search field. All entries that contain these letters are shown in the right pane. Entries that have these letters in their value space are also shown.

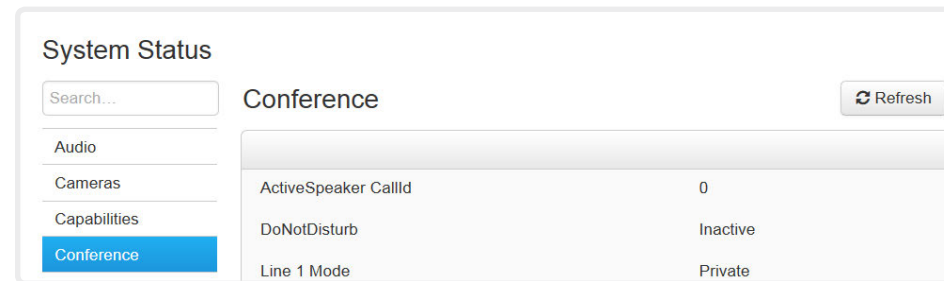


The screenshot shows the 'System Status' interface. On the left, there is a search box containing 'vol' and a list of categories: Audio, Cameras, Capabilities, and Conference. The 'Audio' category is selected. On the right, the 'Audio' status is displayed in a table.

Audio	
Volume	50
VolumeMute	Off

Select a category and navigate to the correct status

The system status is grouped in categories. Choose a category in the left pane to show the related status to the right.



The screenshot shows the 'System Status' interface. On the left, there is a search box and a list of categories: Audio, Cameras, Capabilities, and Conference. The 'Conference' category is selected. On the right, the 'Conference' status is displayed in a table.

Conference	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private

* The status shown in the illustration serve as an example. The status of your system may be different.

Run diagnostics

Sign in to the web interface and navigate to [Diagnostics > Troubleshooting](#).

The troubleshooting page lists the status for some common sources of errors. The list may be different for different products and installations*.

Errors and critical issues are clearly marked in red color; warnings are yellow.

Run diagnostics

Click Re-run diagnostics to ensure that the list is up to date.

Leave standby mode

If the video system is in standby mode, you must click [Deactivate standby](#) to wake up the system.

Troubleshooting Deactivate standby Re-run diagnostics

Diagnostics that helps to identify issues that may cause the TelePresence system to underperform or fail to work as expected.

CRITICAL: Passphrases
There is one or more users without a passphrase set. Please [set a passphrase for all users](#).

WARNING: System Name
The system has not been configured with a name. Please [configure a system name](#). Note that changing the name of the system requires a reboot.

OK: System Temperature
The system is running at an acceptable temperature.

OK: Standby Control
The system goes into standby automatically after 10 minutes. Standby can be configured through the system configuration.

* The messages shown in the illustration serve as examples. Your system may show other information.

Download log files

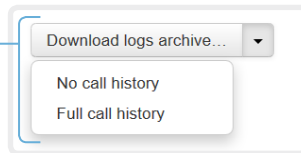
Sign in to the web interface and navigate to [Diagnostics > Log Files](#).

Download all log files

Click [Download logs archive...](#) and follow the instructions.

An anonymized call history is included in the log files by default.

Use the drop down list if you want to exclude the call history from the log files, or if you want to include the full call history (non-anonymous caller/callee).



Open/save one log file

Click the file name to open the log file in the web browser; right click to save the file on the computer.

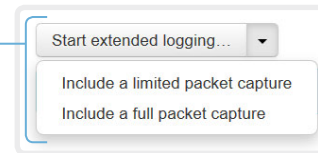
Start extended logging

Click [Start extended logging...](#)

Extended logging lasts for 3 or 10 minutes, depending on whether full capture of network traffic is included or not.

Click [Stop extended logging](#) if you want to stop the extended logging before it times out.

As default, the network traffic is not captured. Use the drop down menu if you want to include partial or full capture of network traffic.



Refresh a log file list

Click the refresh button for *Current logs* or *Historical logs* to update the corresponding lists.



About log files

The log files are Cisco specific debug files which may be requested by the Cisco support organization if you need technical support.

The *current log files* are time stamped event log files.

All current log files are archived in a time stamped *historical log file* each time the video system restarts. If the maximum number of historical log files is reached, the oldest one will be overwritten.


Extended logging mode

Extended logging mode may be switched on to help diagnose network issues and problems during call setup. While in this mode more information is stored in the log files.

Extended logging uses more of the video system's resources, and may cause the video system to under-perform. Only use extended logging mode when you are troubleshooting an issue.

Create a remote support user

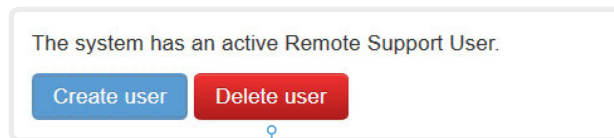
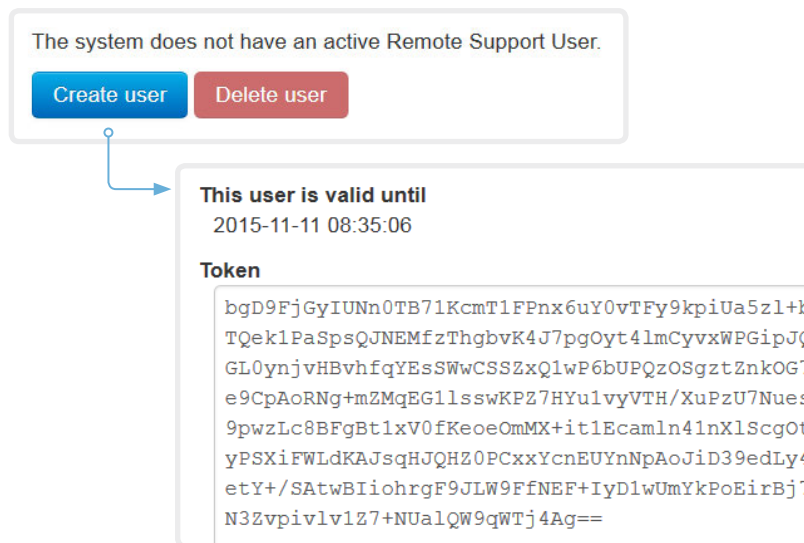
Sign in to the web interface, navigate to [Maintenance > System Recovery](#) and select the *Remote Support User* tab.

 The remote support user should only be enabled for troubleshooting reasons when instructed by Cisco TAC.

Create remote support user

1. Click [Create user](#).
2. Open a case with Cisco TAC.
3. Copy the text in the *Token* field and send it to Cisco TAC.
4. Cisco TAC will generate a *password*.

The remote support user is valid for seven days, or until it is deleted.



Delete remote support user

Click [Delete user](#).

About the remote support user

In cases where you need to diagnose problems on the video system you can create a remote support user.

The remote support user is granted read access to the system and has access to a limited set of commands that can aid troubleshooting.

You will need assistance from Cisco Technical Assistance Center (TAC) to acquire the password for the remote support user.

Backup or restore a configuration

Sign in to the web interface and navigate to [Maintenance > Backup and Restore](#).

Show the current configuration

Click [Preview backup](#) to display the current settings on-screen.

Back up the current configuration

Click [Take backup](#) to store the configuration as a text file.

Restore configuration from backup

1. Click [Browse...](#) and find the backup file with the configuration you want to restore.
2. Click [Restore](#) to reconfigure the system as defined in the file.
Some settings require that you restart the video system before they take effect.

About configuration backup

All the system settings, which are available on the System configuration page, can be listed on-screen or stored as a backup text file.

The backup text file can be loaded back onto the system, thereby restoring the configuration.



We do not recommend that you load back a backup text file from TC software, onto a video system that is running CE software.

The configuration of the video system is likely to be incomplete, due to the differences between the two software generations.

Revert to the previously used software image

Sign in to the web interface and navigate to [Maintenance > System Recovery](#).

We recommend you to back up the log files and configuration of the video system before you swap to the previously used software image.

Back up log files and system configuration

1. Select the *Backup* tab.
2. Click [Download Logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download Configuration Backup](#) and follow the instructions to save the configuration file on your computer.

Revert to the previously used software image

Only administrators, or when in contact with Cisco technical support, should perform this procedure.

1. Select the *Software Recovery Swap* tab.
2. Click [Switch to software: cex.y.z...](#), where x.y.z indicates the software version.
3. Click [Yes](#) to confirm your choice, or [Cancel](#) if you have changed your mind.

Wait while the system resets. The system restarts automatically when finished. This procedure may take a few minutes.


About the previously used software image

If there is a severe problem with the video system, switching to the previously used software image may help solving the problem.

If the system has not been factory reset since the last software upgrade, the previously used software image still resides on the system. You do not have to download the software again.

Factory reset the video system (page 1 of 2)

If there is a severe problem with the video system, the last resort may be to reset it to its default factory settings.

 It is not possible to undo a factory reset.

Always consider reverting to the previously used software image before performing a factory reset. In many situations this will recover the system. Read about software swapping in the ► [Revert to the previously used software image](#) chapter.

We recommend that you use the web interface to factory reset the video system. If the web interface is not available, use the shutdown button.

A factory reset implies:

- Call logs are deleted.
- Passphrases are reset to default.
- All system parameters are reset to default values.
- All files that have been uploaded to the system are deleted. This includes, but is not limited to, custom wallpaper, certificates, local contacts and favorites lists.
- The previous (inactive) software image is deleted.
- Option keys are not affected.

The video system restarts automatically after the factory reset. It is using the same software image as before.

We recommend that you back up the log files and configuration of the video system before you perform a factory reset; otherwise these data will be lost.

Back up log files and system configuration

Sign in to the web interface and navigate to [Maintenance > System Recovery](#).

Back up log files and system configuration

1. Select the *Backup* tab.
2. Click [Download Logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download Configuration Backup](#) and follow the instructions to save the configuration file on your computer.

Factory reset using the web interface

We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.

Sign in to the web interface and navigate to [Maintenance > System Recovery](#).

1. Select the *Factory Reset* tab, and read the provided information carefully
2. Click [Perform a factory reset...](#)
3. Click [Yes](#) to confirm your choice, or [Cancel](#) if you have changed your mind.
4. Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

The video system confirms the factory reset by displaying a notification on the main screen. The notification disappears after approximately 10 seconds.


Factory reset the video system (page 2 of 2)

Factory reset using the shutdown button

We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.

1. Press and hold the shutdown button until the LEDs go out (approximately 5 sec) and the system shuts down.
2. Press and hold the shutdown button until the power LED start blinking (approximately 10 seconds). Then release the button.
3. Within four seconds after the LED starts blinking, press the shutdown button twice to engage the factory reset.
4. Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

The video system confirms the factory reset by displaying a notification on the main screen. The notification disappears after approximately 10 seconds.


-  If you failed to press the shutdown button twice within the four seconds, the system will not revert to the default factory settings, and you will not see the confirmation message. If this happens, go back to step 1 and try again.



Factory reset the Touch 10

In an error situation it may be required to factory reset the Touch controller to recover connectivity. This should be done only when in contact with the Cisco support organization.

When factory resetting the Touch controller the pairing information is lost, and the Touch itself (not the video system) is reverted to factory defaults.

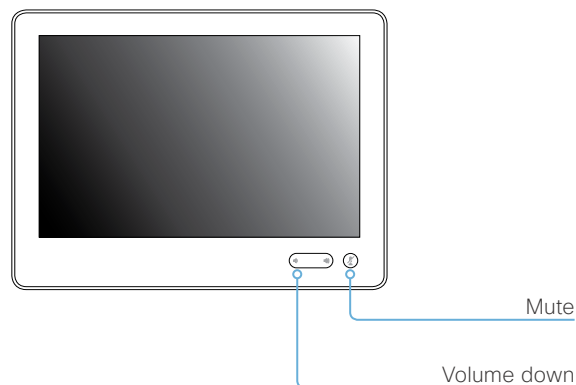
 It is not possible to undo a factory reset.

1. Locate the *Mute* and *Volume down* buttons.
2. Press and hold the *Mute* button until it starts blinking (red and green). It takes approximately 10 seconds.
3. Press the *Volume down* button twice.

Touch 10 automatically reverts to the default factory settings and restarts.

If Touch 10 is directly connected to the video system it receives a new configuration automatically from the video system.

If Touch 10 is connected via LAN the device must be paired to the video system anew. When successfully paired it receives a new configuration automatically from the video system.



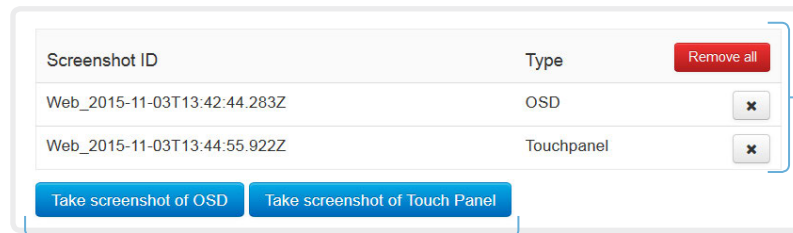
About pairing and how to connect Touch 10 to the video system

In order to use the Touch 10 controller, Touch 10 must either be directly connected to the codec, or paired to the codec via LAN. The latter is referred to as remote pairing.

Read about pairing and how to connect Touch 10 to the video system in the [Connect the Touch 10 controller](#) chapter.

Capture user interface screenshots

Sign in to the web interface and navigate to [Diagnostics > User Interface Screenshots](#).



Capture a screenshot

Click [Take screenshot of Touch Panel](#) to capture a screenshot of the Touch controller, or click [Take screenshot of OSD](#) to capture a screenshot of the on-screen display.

The screenshot displays in the area below the buttons. It may take up to 30 seconds before the screenshot is ready.

All captured snapshots are included in the list above the buttons. Click the screenshot ID to display the image.

Delete screenshots

If you want to delete all screenshots, click [Remove all](#).

To delete just one screenshot, click the button for that screenshot.

About user interface screenshots

You can capture screenshots both of a Touch controller that is connected to the video system, and of the on-screen display (menus, indicators and messages on the main display).



Chapter 5

System settings

Overview of the system settings

In the following pages you will find a complete list of the system settings which are configured from the [System Configuration](#) page on the web interface.

Open a web browser and enter the IP address of the video system then sign in.

How to find the IP address

Tap the contact information in the upper left corner of the Touch controller. Then tap [Settings > System Information](#).

Audio settings	76
Audio DefaultVolume.....	76
Audio Input HDMI [1..3] Level	76
Audio Input HDMI [1..3] Mode	77
Audio Input Line [1..4] Channel.....	77
Audio Input Line [1..4] Equalizer ID	77
Audio Input Line [1..4] Equalizer Mode	77
Audio Input Line [1..4] Level	78
Audio Input Line [1..4] Mode.....	78
Audio Input Line [1..4] VideoAssociation MuteOnInactiveVideo.....	77
Audio Input Line [1..4] VideoAssociation VideoInputSource	77
Audio Input Microphone [1..8] EchoControl Dereverberation.....	78
Audio Input Microphone [1..8] EchoControl Mode	78
Audio Input Microphone [1..8] EchoControl NoiseReduction	78
Audio Input Microphone [1..8] Equalizer ID.....	78
Audio Input Microphone [1..8] Equalizer Mode.....	79
Audio Input Microphone [1..8] Level.....	79
Audio Input Microphone [1..8] Mode	79
Audio Input Microphone [1..8] Type.....	79
Audio Input Microphone [1..8] VideoAssociation MuteOnInactiveVideo	79
Audio Input Microphone [1..8] VideoAssociation VideoInputSource.....	79
Audio Microphones Mute Enabled	76
Audio Output HDMI [1..2] Level	80
Audio Output HDMI [1..2] Mode.....	80
Audio Output Line [1..6] Channel.....	80
Audio Output Line [1..6] Equalizer ID	80
Audio Output Line [1..6] Equalizer Mode	80
Audio Output Line [1..6] Level	80
Audio Output Line [1..6] Mode.....	81
Audio SoundsAndAlerts RingTone.....	76
Audio SoundsAndAlerts RingVolume.....	76
CallHistory settings	82
CallHistory Mode.....	82
Cameras settings	83
Cameras Camera [1..7] AssignedSerialNumber.....	83
Cameras Camera [1..7] Backlight DefaultMode.....	83

Cameras Camera [1..7] Brightness DefaultLevel.....	83	Conference Presentation RelayQuality	92
Cameras Camera [1..7] Brightness Mode	83	Conference VideoBandwidth MainChannel Weight.....	92
Cameras Camera [1..7] Flip	83	Conference VideoBandwidth Mode.....	92
Cameras Camera [1..7] Focus Mode.....	84	Conference VideoBandwidth PresentationChannel Weight	92
Cameras Camera [1..7] Gamma Level.....	84	FacilityService settings.....	93
Cameras Camera [1..7] Gamma Mode	84	FacilityService Service [1..5] CallType	93
Cameras Camera [1..7] Mirror	84	FacilityService Service [1..5] Name.....	93
Cameras Camera [1..7] MotorMoveDetection	84	FacilityService Service [1..5] Number	93
Cameras Camera [1..7] Whitebalance Level	85	FacilityService Service [1..5] Type	93
Cameras Camera [1..7] Whitebalance Mode.....	85	GPIO settings.....	94
Cameras PowerLine Frequency.....	85	GPIO Pin [1..4] Mode	94
Cameras Preset TriggerAutofocus.....	85	H323 settings.....	95
Cameras SpeakerTrack ConnectorDetection CameraLeft.....	86	H323 Authentication LoginName	95
Cameras SpeakerTrack ConnectorDetection CameraRight.....	86	H323 Authentication Mode	95
Cameras SpeakerTrack ConnectorDetection Mode	86	H323 Authentication Password	95
Cameras SpeakerTrack Mode.....	85	H323 CallSetup Mode.....	95
Cameras SpeakerTrack TrackingMode	86	H323 Encryption KeySize.....	96
Cameras SpeakerTrack Whiteboard Mode	87	H323 Gatekeeper Address	96
Conference settings	88	H323 H323Alias E164	96
Conference ActiveControl Mode	88	H323 H323Alias ID.....	96
Conference AutoAnswer Delay.....	88	H323 NAT Address	97
Conference AutoAnswer Mode	88	H323 NAT Mode	96
Conference AutoAnswer Mute	88	H323 PortAllocation.....	97
Conference CallProtocolIPStack.....	88	Logging settings	98
Conference DefaultCall Protocol	89	Logging Mode.....	98
Conference DefaultCall Rate.....	89	Network settings.....	99
Conference DoNotDisturb DefaultTimeout	89	Network [1] DNS Domain Name	99
Conference Encryption Mode	89	Network [1] DNS Server [1..3] Address	99
Conference FarEndControl Mode	89	Network [1] IEEE8021X AnonymousIdentity	100
Conference FarEndControl SignalCapability.....	90	Network [1] IEEE8021X Eap Md5	100
Conference IncomingMultisiteCall Mode	91	Network [1] IEEE8021X Eap Peap.....	101
Conference MaxReceiveCallRate	90	Network [1] IEEE8021X Eap Tls	100
Conference MaxTotalReceiveCallRate	90	Network [1] IEEE8021X Eap Ttls.....	100
Conference MaxTotalTransmitCallRate	90	Network [1] IEEE8021X Identity	100
Conference MaxTransmitCallRate.....	90	Network [1] IEEE8021X Mode.....	99
Conference MicUnmuteOnDisconnect Mode.....	91	Network [1] IEEE8021X Password	100
Conference Multipoint Mode	91	Network [1] IEEE8021X TlsVerify	99
Conference MultiStream Mode.....	91		
Conference Presentation OnPlacedOnHold	92		

Network [1] IEEE8021X UseClientCertificate.....	99	NetworkServices SNMP SystemLocation	108
Network [1] IPStack	101	NetworkServices SSH AllowPublicKey	109
Network [1] IPv4 Address.....	101	NetworkServices SSH Mode	109
Network [1] IPv4 Assignment	101	NetworkServices Telnet Mode.....	109
Network [1] IPv4 Gateway	101	NetworkServices UPnP Mode	109
Network [1] IPv4 SubnetMask	101	NetworkServices UPnP Timeout	109
Network [1] IPv6 Address.....	102	NetworkServices WelcomeText	110
Network [1] IPv6 Assignment	102	NetworkServices XMLAPI Mode	110
Network [1] IPv6 DHCPOptions.....	102	Peripherals settings	111
Network [1] IPv6 Gateway	102	Peripherals Pairing CiscoTouchPanels RemotePairing	111
Network [1] MTU.....	102	Peripherals Pairing Ultrasound Volume MaxLevel	111
Network [1] QoS Diffserv Audio	103	Peripherals Pairing Ultrasound Volume Mode	111
Network [1] QoS Diffserv Data	103	Peripherals Profile TouchPanels	111
Network [1] QoS Diffserv ICMPv6.....	104	Phonebook settings	112
Network [1] QoS Diffserv NTP.....	104	Phonebook Server [1] ID	112
Network [1] QoS Diffserv Signalling	103	Phonebook Server [1] Type	112
Network [1] QoS Diffserv Video	103	Phonebook Server [1] URL	112
Network [1] QoS Mode.....	102	Provisioning settings.....	113
Network [1] RemoteAccess Allow	104	Provisioning Connectivity.....	113
Network [1] Speed.....	104	Provisioning ExternalManager Address	114
Network [1] TrafficControl Mode	105	Provisioning ExternalManager AlternateAddress.....	114
Network [1] VLAN Voice Mode.....	105	Provisioning ExternalManager Domain	114
Network [1] VLAN Voice VlanId	105	Provisioning ExternalManager Path	114
NetworkServices settings	106	Provisioning ExternalManager Protocol	114
NetworkServices CDP Mode	106	Provisioning HttpMethod	113
NetworkServices H323 Mode	106	Provisioning LoginName	113
NetworkServices HTTP Mode	106	Provisioning Mode	113
NetworkServices HTTPS OCSP Mode	107	Provisioning Password.....	113
NetworkServices HTTPS OCSP URL	107	Proximity settings	115
NetworkServices HTTPS VerifyClientCertificate	107	Proximity Mode	115
NetworkServices HTTPS VerifyServerCertificate	106	Proximity Services CallControl	115
NetworkServices NTP Mode	107	Proximity Services ContentShare FromClients.....	115
NetworkServices NTP Server [1..3] Address	107	Proximity Services ContentShare ToClients	115
NetworkServices SIP Mode.....	107	RTP settings.....	116
NetworkServices SNMP CommunityName	108	RTP Ports Range Start.....	116
NetworkServices SNMP Host [1..3] Address	108	RTP Ports Range Stop	116
NetworkServices SNMP Mode.....	108		
NetworkServices SNMP SystemContact.....	108		

Security settings	117	Standby Delay.....	124
Security Audit Logging Mode.....	117	Standby StandbyAction.....	124
Security Audit OnError Action.....	117	Standby WakeupAction.....	124
Security Audit Server Address.....	117		
Security Audit Server Port.....	118	SystemUnit settings	125
Security Audit Server PortAssignment.....	118	SystemUnit Name.....	125
Security Session InactivityTimeout.....	118		
Security Session ShowLastLogon.....	118	Time settings	126
		Time DateFormat.....	126
SerialPort settings	119	Time TimeFormat.....	126
SerialPort BaudRate.....	119	Time Zone.....	127
SerialPort LoginRequired.....	119		
SerialPort Mode.....	119	UserInterface settings	129
		UserInterface ContactInfo Type.....	129
SIP settings	120	UserInterface KeyTones Mode.....	129
SIP ANAT.....	120	UserInterface Language.....	129
SIP Authentication Password.....	120	UserInterface OSD EncryptionIndicator.....	129
SIP Authentication UserName.....	120	UserInterface OSD Output.....	130
SIP DefaultTransport.....	120	UserInterface UserPreferences.....	130
SIP DisplayName.....	120	UserInterface Wallpaper.....	130
SIP Ice DefaultCandidate.....	121		
SIP Ice Mode.....	121	Video settings	131
SIP Line.....	121	Video ActiveSpeaker DefaultPIPPosition.....	131
SIP ListenPort.....	121	Video DefaultLayoutFamily Local.....	131
SIP Mailbox.....	121	Video DefaultLayoutFamily Remote.....	132
SIP PreferredIPMedia.....	122	Video DefaultMainSource.....	132
SIP PreferredIPSignaling.....	122	Video Input Connector [1..4] PresentationSelection.....	134
SIP Proxy [1..4] Address.....	122	Video Input Connector [1..4] RGBQuantizationRange.....	135
SIP TlsVerify.....	122	Video Input Connector [1..5] CameraControl Camerald.....	132
SIP Turn BandwidthProbe.....	122	Video Input Connector [1..5] CameraControl Mode.....	132
SIP Turn DiscoverMode.....	122	Video Input Connector [1..5] InputSourceType.....	133
SIP Turn DropRflx.....	123	Video Input Connector [1..5] Name.....	133
SIP Turn Password.....	123	Video Input Connector [1..5] OptimalDefinition Profile.....	134
SIP Turn Server.....	123	Video Input Connector [1..5] OptimalDefinition Threshold60fps.....	134
SIP Turn UserName.....	123	Video Input Connector [1..5] Quality.....	133
SIP Type.....	123	Video Input Connector [1..5] Visibility.....	135
SIP URI.....	123	Video Input Connector [4] DviType.....	133
		Video Input Connector [5] SignalType.....	133
Standby settings	124	Video Monitors.....	135
Standby BootAction.....	124	Video Output Connector [1..2] CEC Mode.....	136
Standby Control.....	124	Video Output Connector [1..3] Location HorizontalOffset.....	136

Video Output Connector [1..3] Location VerticalOffset.....	137
Video Output Connector [1..3] MonitorRole	137
Video Output Connector [1..3] Resolution.....	137
Video Output Connector [1..3] RGBQuantizationRange.....	138
Video Presentation DefaultPIPPosition	138
Video Presentation DefaultSource.....	138
Video Selfview Default FullscreenMode	139
Video Selfview Default Mode.....	138
Video Selfview Default OnMonitorRole.....	139
Video Selfview Default PIPPosition.....	139
Video Selfview OnCall Duration.....	140
Video Selfview OnCall Mode	139
Experimental settings	141

Audio settings

Audio DefaultVolume

Define the default volume for the speakers. The volume is set to this value when you switch on or restart the video system. Use the Touch controller to change the volume while the video system is running. You may also use API commands (xCommand Audio Volume) to change the volume while the video system is running, and to reset to default value.

Requires user role: USER

Default value: 50

Value space: Integer (0..100)

Select a value between 1 and 100. This corresponds to the dB range from -34.5 dB to 15 dB, in steps of 0.5 dB). If set to 0 the audio is switched off.

Audio Microphones Mute Enabled

Define the microphone mute behaviour on the video system.

Requires user role: ADMIN

Default value: True

Value space: True/InCallOnly

True: Muting of audio is always available.

InCallOnly: Muting of audio is only available when the device is in a call. When Idle it is not possible to mute the microphone. This is useful when an external telephone service/ audio system is connected via the codec and is to be available when the codec is not in a call. When set to InCallOnly this will prevent the audio-system from being muted by mistake.

Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: USER

Default value: Sunrise

Value space: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

Select a ringtone from the list.

Audio SoundsAndAlerts RingVolume

Define the ring volume for incoming calls.

Requires user role: USER

Default value: 50

Value space: Integer (0..100)

The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Volume 0 = Off.

Audio Input HDMI [1..3] Level

Define the audio level of the HDMI input connector.

Requires user role: ADMIN

Default value: 0

Value space: Integer (-24..0)

Select a value between -24 and 0, in steps of 1 dB.

Audio Input HDMI [1..3] Mode

Define if the audio channels on the HDMI input shall be enabled. The HDMI inputs have two audio channels.

Requires user role: ADMIN

Default value: HDMI [1..2]: Off HDMI [3]: On

Value space: Off/On

- Off: Disable audio on the HDMI input.
- On: Enable audio on the HDMI input.

Audio Input Line [1..4] Equalizer ID

Select the equalizer ID of the audio source that is connected to the line input.

Requires user role: ADMIN

Default value: 1

Value space: Integer (1..8)

- Set the equalizer ID.

Audio Input Line [1..4] Equalizer Mode

Define the equalizer mode for the audio source that is connected to the line input.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

- Off: No equalizer.
- On: Enable the equalizer for the audio source that is connected to the line input.

Audio Input Line [1..4] VideoAssociation MuteOnInactiveVideo

The audio source can be associated with a video source on the video input connector, and you can determine whether to play or mute audio depending on whether the video source is presented or not. By default, audio is not muted.

Requires user role: ADMIN

Default value: Line [1, 2]: On Line[3, 4]: Off

Value space: Off/On

Off: The audio source is not associated with a video source. The audio will be played locally and to far end regardless of whether the video source is presented.

On: The audio source is associated with a video source. The audio will be played (locally and to far end) when the associated video source is presented. The audio will be muted when the video source is not presented.

Audio Input Line [1..4] VideoAssociation VideoInputSource

The audio source can be associated with a video source on the video input connector.

Requires user role: ADMIN

Default value: Line [1, 2]: 4 Line[3, 4]: 1

Value space: 1/2/3/4/5

Select the video input connector to associate the audio source with.

Audio Input Line [1..4] Channel

Define whether the audio source on the line input is a mono signal or part of a multichannel signal.

Requires user role: ADMIN

Default value: Left

Value space: Left/Mono/Right

Left: The Audio Line input signal is the left channel of a stereo signal.

Mono: The Audio Line input signal is a mono signal.

Right: The Audio Line input signal is the right channel of a stereo signal.

Audio Input Line [1..4] Level

Define the level of the audio source on the line input connector.

See the Audio Level table in the Physical Interface Guide for the codec for a complete overview of the values represented in dB.

Requires user role: ADMIN

Default value: 10

Value space: Integer (0..24)

Select a value between 0 and 24, in steps of 1 dB.

Audio Input Line [1..4] Mode

Define the mode for the audio input line.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the Audio Line input.

On: Enable the Audio Line input.

Audio Input Microphone [1..8] EchoControl Mode

The echo canceller continuously adjusts itself to the audio characteristics of the room and compensate for any changes it detects in the audio environment. If the changes in the audio conditions are very significant the echo canceller may take a second or two to re-adjust.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Echo Control should be switched Off if external echo cancellation or playback equipment is used.

On: Echo Control is normally set to On to prevent the far end from hearing their own audio. Once selected, echo cancellation is active at all times.

Audio Input Microphone [1..8] EchoControl NoiseReduction

The system has a built-in noise reduction which reduces constant background noise (for example noise from air-conditioning systems, cooling fans etc.). In addition, a high pass filter (Humfilter) reduces very low frequency noise. Requires the Echo Control Mode to be enabled for the microphone.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Turn off the Noise Reduction.

On: The Noise Reduction should be enabled in the presence of low frequency noise.

Audio Input Microphone [1..8] EchoControl Dereverberation

The system has built-in signal processing to reduce the effect of room reverberation. Requires the Echo Control Mode to be enabled for the microphone.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

Audio Input Microphone [1..8] Equalizer ID

Select the equalizer ID of the source that is connected to the microphone input.

Requires user role: ADMIN

Default value: 1

Value space: Integer (1..8)

Set the equalizer ID.

Audio Input Microphone [1..8] Equalizer Mode

Define the equalizer mode for the source that is connected to the microphone input.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: No equalizer.

On: Enable the equalizer for the source that is connected to the microphone input.

Audio Input Microphone [1..8] VideoAssociation MuteOnInactiveVideo

The microphone can be associated with a video source on the video input connector, and you can determine whether to play or mute audio depending on whether the video source is presented or not. By default, audio is not muted.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: No video source is associated.

On: A video source is associated, and the audio will be muted if the associated video source is not displayed.

Audio Input Microphone [1..8] VideoAssociation VideoInputSource

Select the video input connector to associate the audio source with.

Requires user role: ADMIN

Default value: 1

Value space: 1/2/3/4/5

Select the video input connector to associate the audio source with.

Audio Input Microphone [1..8] Level

Define the audio level of the Microphone input connector.

See the Audio Level table in the Physical Interface Guide for the codec for a complete overview of the values represented in dB.

Requires user role: ADMIN

Default value: 58

Value space: Integer (0..70)

Select a value between 0 and 70, in steps of 1 dB.

Audio Input Microphone [1..8] Mode

Define the audio input microphone mode.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the audio input microphone connector.

On: Enable the audio input microphone connector.

Audio Input Microphone [1..8] Type

The microphone connectors are intended for electret type microphones. The microphone connector can be set to line or microphone mode.

Requires user role: ADMIN

Default value: Line

Value space: Line/Microphone

Microphone: Select Microphone when you have 48 V Phantom voltage and the pre-amplification is On.

Line: Select Line when you have a standard balanced line input. The phantom voltage and pre-amplification is Off.

Audio Output HDMI [1..2] Level

Define the output level of the HDMI output connector, in steps of 1 dB.

Requires user role: ADMIN

Default value: 0

Value space: Integer (-24..0)

Select a value between -24 and 0, in steps of 1 dB.

Audio Output HDMI [1..2] Mode

Define if the audio channel on the HDMI output connector shall be enabled.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the audio channel on the HDMI output.

On: Enable the audio channel on the HDMI output.

Audio Output Line [1..6] Channel

Define whether the Audio Line output is a mono signal or part of a multichannel signal.

Requires user role: ADMIN

Default value: Left

Value space: Left/Mono/Right

Left: The Audio Line output signal is the left channel of a stereo signal.

Mono: The Audio Line output signal is a mono signal.

Right: The Audio Line output signal is the right channel of a stereo signal.

Audio Output Line [1..6] Equalizer ID

Select the equalizer ID for the audio source that is connected to the output line.

Requires user role: ADMIN

Default value: 1

Value space: Integer (1..8)

Set the equalizer ID.

Audio Output Line [1..6] Equalizer Mode

Define the equalizer mode for the audio source that is connected to the output line.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: No equalizer.

On: Enable the equalizer for the audio output line.

Audio Output Line [1..6] Level

Define the audio level on the line output connector.

See the Audio Level table in the Physical Interface Guide for the codec for a complete overview of the menu values represented in dB.

Requires user role: ADMIN

Default value: -10

Value space: Integer (-24..0)

Select a value between -24 and 0, in steps of 1 dB.

Audio Output Line [1..6] Mode

Define the mode for the audio output line.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the audio output line.

On: Enable the audio output line.

CallHistory settings

CallHistory Mode

Determine whether or not information about calls that are placed or received are stored, including missed calls and calls that are not answered (call history). This determines whether or not the calls appear in the Recents list in the user interfaces.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: New entries are not added to the call history.

On: New entries are stored in the call history list.

Cameras settings

Cameras Camera [1..7] AssignedSerialNumber

The camera ID is the number *n* in Camera [*n*]. By default, the camera ID is assigned automatically to a camera. If EDID information is not passed on from the camera to the codec, the camera ID is not persistent after a reboot. This means that a camera may get a new camera ID when the codec (video system) is restarted.

You should use the Cameras Camera AssignedSerialNumber setting to cater for configurations where the codec does not receive EDID information from multiple cameras. This setting allows you to manually assign a camera ID to a camera by associating the camera ID with the camera's serial number. The setting is persistent until the codec is factory reset.

Typical situations where the codec does not receive EDID information are: when you connect a Cisco TelePresence 60 camera using 3G-SDI; when you connect a Cisco TelePresence 60 (Cisco PrecisionHD 1080p4xS2) camera; when you use an HDMI repeater that does not pass on EDID information.

The default value is an empty string.

Requires user role: USER

Default value: ""

Value space: String (0, 20)

The camera's serial number.

Cameras Camera [1..7] Backlight DefaultMode

This configuration turns backlight compensation on or off. Backlight compensation is useful when there is much light behind the persons in the room. Without compensation the persons will easily appear very dark to the far end.

Requires user role: USER

Default value: Off

Value space: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Cameras Camera [1..7] Brightness Mode

Define the camera brightness mode.

Requires user role: USER

Default value: Auto

Value space: Auto/Manual

Auto: The camera brightness is automatically set by the system.

Manual: Enable manual control of the camera brightness. The brightness level is set using the Cameras Camera [*n*] Brightness DefaultLevel setting.

Cameras Camera [1..7] Brightness DefaultLevel

Define the brightness level. Requires the Cameras Camera [*n*] Brightness Mode to be set to Manual.

Requires user role: USER

Default value: 20

Value space: Integer (1..31)

The brightness level.

Cameras Camera [1..7] Flip

With Flip mode (vertical flip) you can flip the image upside down. Flipping applies both to the self-view and the video that is transmitted to the far end.

Requires user role: USER

Default value: Auto

Value space: Auto/Off/On

Auto: If the camera detects that it is mounted upside down, the image is automatically flipped. If the camera cannot auto-detect whether it is mounted upside down or not, the image is not changed.

Off: Display the image on screen the normal way.

On: Display the image flipped upside down. This setting is used when a camera is mounted upside down, but cannot automatically detect which way it is mounted.

Cameras Camera [1..7] Focus Mode

Define the camera focus mode.

Requires user role: USER

Default value: Auto

Value space: Auto/Manual

Auto: The camera will auto focus once a call is connected, as well as after moving the camera (pan, tilt, zoom). The system will use auto focus only for a few seconds to set the right focus; then auto focus is turned off to prevent continuous focus adjustments of the camera.

Manual: Turn the autofocus off and adjust the camera focus manually.

Cameras Camera [1..7] Gamma Mode

This setting enables gamma corrections, and applies only to cameras which support gamma mode. Gamma describes the nonlinear relationship between image pixels and monitor brightness.

Requires user role: USER

Default value: Auto

Value space: Auto/Manual

Auto: Auto is the default and the recommended setting.

Manual: In manual mode the gamma value is changed with the gamma level setting, ref. Cameras Camera [n] Gamma Level.

Cameras Camera [1..7] Gamma Level

By setting the Gamma Level you can select which gamma correction table to use. This setting may be useful in difficult lighting conditions, where changes to the brightness setting does not provide satisfactory results. Requires the Cameras Camera [n] Gamma Mode to be set to Manual.

Requires user role: USER

Default value: 0

Value space: Integer (0..7)

Define the gamma level.

Cameras Camera [1..7] Mirror

With Mirror mode (horizontal flip) you can mirror the image on screen. Mirroring applies both to the self-view and the video that is transmitted to the far end

Requires user role: USER

Default value: Auto

Value space: Auto/Off/On

Auto: If the camera detects that it is mounted upside down, the image is automatically mirrored. If the camera cannot auto-detect whether it is mounted upside down or not, the image is not changed.

Off: Display the image as other people see you.

On: Display the image as you see yourself in a mirror.

Cameras Camera [1..7] MotorMoveDetection

This setting applies only when using a Cisco TelePresence PrecisionHD 1080p12x camera.

If adjusting the camera position by hand you can configure whether the camera should keep its new position or return to the preset or position it had before.

Requires user role: USER

Default value: Off

Value space: Off/On

Off: When the camera position is adjusted manually the camera will keep this position until adjusted again. **WARNING:** If moving the camera by hand, the camera will not register the new pan and tilt values since there is no position feedback. This will result in wrong pan and tilt values when recalling the camera presets subsequently.

On: When the camera position is adjusted manually, or the camera detects that the motors have moved, it will first re-initialize (i.e. go to default position) then return to the preset/position it had before the camera was adjusted.

Cameras Camera [1..7] Whitebalance Mode

Define the camera white balance mode.

Requires user role: USER

Default value: Auto

Value space: Auto/Manual

Auto: The camera will continuously adjust the white balance depending on the camera view.

Manual: Enables manual control of the camera white balance. The white balance level is set using the Cameras Camera [n] Whitebalance Level setting.

Cameras Camera [1..7] Whitebalance Level

Define the white balance level. Requires the Cameras Camera [n] Whitebalance Mode to be set to manual.

Requires user role: USER

Default value: 1

Value space: Integer (1..16)

The white balance level.

Cameras PowerLine Frequency

If your camera supports power line frequency anti-flickering, the camera is able to compensate for any flicker noise from the electrical power supply. You should set this camera configuration based on your power line frequency. If your camera supports auto detection of line frequency, you can select the Auto option in the configuration.

All Cisco Precision cameras support both anti-flickering and auto detection of line frequency. Auto is the default value, so you should change this setting if you have a camera that does not support auto detection.

Requires user role: ADMIN

Default value: Auto

Value space: 50Hz/60Hz/Auto

50Hz: Use this value when the power line frequency is 50 Hz.

60Hz: Use this value when the power line frequency is 60 Hz.

Auto: Allow the camera to detect the power frequency automatically.

Cameras Preset TriggerAutofocus

The current position (pan and tilt), zoom and focus are stored with a preset. Use this setting to determine if the camera should refocus or use the focus value that is stored with the preset.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

Auto: Whether the camera refocuses or not when selecting a preset, depends on the camera type.

Off: The focus value that is stored with the preset will be used. The camera will not refocus when selecting a preset.

On: The camera will refocus when selecting a preset. The focus value that is stored with the preset may be overridden.

Cameras SpeakerTrack Mode

This setting applies only when using a Cisco TelePresence SpeakerTrack 60 camera.

The SpeakerTrack 60 camera assembly consists of two cameras and uses an audio tracking technique that finds and captures a close-up of the active speaker. When a change of speaker is detected, the system can switch automatically between the two cameras to always show the best camera view. Refer to the Cameras SpeakerTrack TrackingMode setting for different switching modes.

Requires user role: USER

Default value: Auto

Value space: Auto/Off

Auto: Speaker tracking is switched on. The cameras in the camera assembly behave as one integrated unit that finds the active speaker and dynamically chooses the best camera view.

Off: The cameras operate as two individual cameras. Speaker tracking is not used.

Cameras SpeakerTrack TrackingMode

This setting applies only when using a Cisco TelePresence SpeakerTrack 60 camera, and when Cameras SpeakerTrack Mode is set to Auto.

The speaker tracking algorithm can react to changes in two modes, one faster than the other. The mode determines when the camera view will change to a new speaker.

Requires user role: USER

Default value: Auto

Value space: Auto/Conservative

Auto: Normal tracking mode.

Conservative: The camera view will change to a new speaker later than in Normal mode.

Cameras SpeakerTrack ConnectorDetection Mode

This setting applies only when a Cisco TelePresence SpeakerTrack 60 camera is connected to the codec (video system).

Define whether to automatically detect or manually configure which video input each individual camera is connected to. You should choose manual configuration in situations where the codec does not receive EDID information from the cameras. Typically, this will be when you use HDMI repeaters that do not pass on EDID information.

Requires user role: USER

Default value: Auto

Value space: Auto/Manual

Auto: Automatically detect which video inputs the cameras are connected to.

Manual: Manually define which video inputs the cameras are connected to. Use the Cameras SpeakerTrack ConnectorDetection CameraLeft and Cameras SpeakerTrack ConnectorDetection CameraRight settings.

Cameras SpeakerTrack ConnectorDetection CameraLeft

This setting applies only when a Cisco TelePresence SpeakerTrack 60 camera is connected to the codec (video system). Furthermore, Cameras SpeakerTrack ConnectorDetection Mode must be set to Manual.

Define the number of the video input that SpeakerTrack 60's left camera is connected to.

Requires user role: USER

Default value: 1

Value space: Integer (1..5)

Set a valid video input number. For example, set to 1 if the left camera is connected to video input 1.

Cameras SpeakerTrack ConnectorDetection CameraRight

This setting applies only when a Cisco TelePresence SpeakerTrack 60 camera is connected to the codec (video system). Furthermore, Cameras SpeakerTrack ConnectorDetection Mode must be set to Manual.

Define the number of the video input that SpeakerTrack 60's right camera is connected to.

Requires user role: USER

Default value: 2

Value space: Integer (1..5)

Set a valid video input number. For example, set to 2 if the right camera is connected to video input 2.

Cameras SpeakerTrack Whiteboard Mode

This setting applies only when a Cisco TelePresence SpeakerTrack 60 camera is connected to the codec.

Define whether to enable the Snap to Whiteboard feature or not.

The Snap to Whiteboard feature relies on a speaker track camera. When a presenter is standing next to the whiteboard, the camera will capture both the presenter and the whiteboard if the Snap to Whiteboard feature is enabled. If the feature is disabled, only the presenter will be captured.

The Snap to Whiteboard feature is set up from the Touch controller.

Requires user role: USER

Default value: Off

Value space: Off/On

Off: The Snap to Whiteboard feature is disabled.

On: The Snap to Whiteboard feature is enabled.

Conference settings

Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server using the video system's interfaces. Each user can see the participant list, change video layout, disconnect participants, etc. from the interface. The active control feature is enabled by default, provided that it is supported by the infrastructure (Cisco Unified Communications Manager (CUCM) version 9.1.2 or newer, Cisco TelePresence Video Communication Server (VCS) version X8.1 or newer). Change this setting if you want to disable the active control features.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off

Auto: Active control is enabled when supported by the infrastructure.

Off: Active control is disabled.

Conference AutoAnswer Mode

Define the auto answer mode. Use the Conference AutoAnswer Delay setting if you want the system to wait a number of seconds before answering the call, and use the Conference AutoAnswer Mute setting if you want your microphone to be muted when the call is answered.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: You must answer incoming calls manually by tapping Answer on the Touch controller.

On: The system automatically answers incoming calls, except if you are already in a call. You must always answer or decline incoming calls manually when you are already engaged in a call.

Conference AutoAnswer Mute

Define if the microphone shall be muted when an incoming call is automatically answered. Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The incoming call will not be muted.

On: The incoming call will be muted when automatically answered.

Conference AutoAnswer Delay

Define how long (in seconds) an incoming call has to wait before it is answered automatically by the system. Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..50)

The auto answer delay (seconds).

Conference CallProtocolIPStack

Select if the system should enable IPv4, IPv6, or dual IP stack on the call protocol (SIP, H323).

Requires user role: ADMIN

Default value: Dual

Value space: Dual/IPv4/IPv6

Dual: Enables both IPv4 and IPv6 for the call protocol.

IPv4: When set to IPv4, the call protocol will use IPv4.

IPv6: When set to IPv6, the call protocol will use IPv6.

Conference DefaultCall Protocol

Define the Default Call Protocol to be used when placing calls from the system.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/H323/Sip/H320

Auto: Enables auto-selection of the call protocol based on which protocols are available. If multiple protocols are available, the order of priority is: 1) SIP; 2) H323; 3) H320. If the system cannot register, or the call protocol is not enabled, the auto-selection chooses H323.

H323: All calls are set up as H.323 calls.

Sip: All calls are set up as SIP calls.

H320: All calls are set up as H.320 calls (only applicable if connected to Cisco TelePresence ISDN Link).

Conference DefaultCall Rate

Define the Default Call Rate to be used when placing calls from the system.

Requires user role: ADMIN

Default value: 1920

Value space: Integer (64..6000)

Set the default call rate (kbps).

Conference DoNotDisturb DefaultTimeout

This setting determines the default duration of a Do Not Disturb session, i.e. the period when incoming calls are rejected and registered as missed calls. The session can be terminated earlier by using the user interface (Touch controller). The default value is 60 minutes.

Requires user role: ADMIN

Default value: 60

Value space: Integer (0..1440)

Set the number of minutes (between 0 and 1440, i.e. 24 hours) before the Do Not Disturb session times out automatically.

Conference Encryption Mode

Define the conference encryption mode. A padlock with the text "Encryption On" or "Encryption Off" displays on screen for a few seconds when the conference starts.

NOTE: If the Encryption Option Key is not installed on the video system, the encryption mode is always Off.

Requires user role: ADMIN

Default value: BestEffort

Value space: Off/On/BestEffort

Off: The system will not use encryption.

On: The system will only allow calls that are encrypted.

BestEffort: The system will use encryption whenever possible.

> In Point to point calls: If the far end system supports encryption (AES-128), the call will be encrypted. If not, the call will proceed without encryption.

> In MultiSite calls: In order to have encrypted MultiSite conferences, all sites must support encryption. If not, the conference will be unencrypted.

Conference FarEndControl Mode

Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The far end is not allowed to select your video sources or to control your local camera (pan, tilt, zoom).

On: Allows the far end to be able to select your video sources and control your local camera (pan, tilt, zoom). You will still be able to control your camera and select your video sources as normal.

Conference FarEndControl SignalCapability

Define the far end control (H.224) signal capability mode.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

Conference MaxReceiveCallRate

Define the maximum receive bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call; use the Conference MaxTotalReceiveCallRate setting to set the aggregated maximum for all simultaneous active calls.

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

Set the maximum receive call rate (kbps).

Conference MaxTransmitCallRate

Define the maximum transmit bit rate to be used when placing or receiving calls. Note that this is the maximum bit rate for each individual call; use the Conference MaxTotalTransmitCallRate setting to set the aggregated maximum for all simultaneous active calls.

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

Set the maximum transmitt call rate (kbps).

Conference MaxTotalReceiveCallRate

This configuration applies when using a video system's built-in MultiSite feature (optional) to host a multipoint video conference.

Define the maximum overall receive bit rate allowed. The bit rate will be divided fairly among all active calls at any time. This means that the individual calls will be up-speeded or down-speeded as appropriate when someone leaves or enters a multipoint conference, or when a call is put on hold (suspended) or resumed.

The maximum receive bit rate for each individual call is defined in the Conference MaxReceiveCallRate setting.

Requires user role: ADMIN

Default value: 10000

Value space: Integer (64..10000)

Set the maximum receive call rate (kbps).

Conference MaxTotalTransmitCallRate

This configuration applies when using a video system's built-in MultiSite feature (optional) to host a multipoint video conference.

Define the maximum overall transmit bit rate allowed. The bit rate will be divided fairly among all active calls at any time. This means that the individual calls will be up-speeded or down-speeded as appropriate when someone leaves or enters a multipoint conference, or when a call is put on hold (suspended) or resumed.

The maximum transmit bit rate for each individual call is defined in the Conference MaxTransmitCallRate setting.

Requires user role: ADMIN

Default value: 10000

Value space: Integer (64..10000)

Set the maximum transmit call rate (kbps).

Conference MicUnmuteOnDisconnect Mode

Define if the microphones shall be unmuted automatically when all calls are disconnected. In a meeting room or other shared resources this may be done to prepare the system for the next user.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: If muted during a call, let the microphones remain muted after the call is disconnected.

On: Unmute the microphones after the call is disconnected.

Conference Multipoint Mode

Define how the video system handles multiparty video conferences (ad hoc conferences). If registered to a Cisco TelePresence Video Communication Server (VCS), the video system can use its own built-in MultiSite feature. If registered to a Cisco Unified Communications Manager (CUCM) version 8.6.2 or newer, the video system can use either the CUCM conference bridge, or the video system's own built-in MultiSite feature. Which option to use, is set-up by CUCM.

The CUCM conference bridge allows you to set up conferences with many participants. The built-in MultiSite allows up to five participants (yourself included) plus one additional audio call.

The built-in MultiSite is optional and may not be available on all video systems.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/MultiSite/CUCMMediaResourceGroupList

Auto: The multipoint method is chosen automatically; if no multipoint method is available, the Multipoint Mode will be set to Off.

Off: Multiparty conferences are not allowed.

MultiSite: Multiparty conferences are set up using the built-in MultiSite feature. If MultiSite is chosen when the MultiSite feature is not available, the Multipoint Mode will automatically be set to Off.

CUCMMediaResourceGroupList: Multiparty conferences are hosted by the CUCM configured conference bridge. This setting is provisioned by CUCM in a CUCM environment, and should never be set manually by the user.

Conference MultiStream Mode

The video system supports multistream video for conferences, provided that the conference infrastructure supports the feature (Cisco TelePresence Server 4.2 or later). This means that the video system can compose the video streams locally into a conference layout which utilizes all available screens. This results in an enhanced user experience.

Multistream video is supported only via SIP.

Requires user role: ADMIN

Default value: Off

Value space: Auto/Off

Auto: Use local composition of video streams if the feature is supported by the conference infrastructure.

Off: Local composition is disabled. Layouts will be transcoded by the conference infrastructure (Cisco TelePresence Server).

Conference IncomingMultisiteCall Mode

Select whether or not to allow incoming calls when already in a call/conference.

Requires user role: ADMIN

Default value: Allow

Value space: Allow/Deny

Allow: You will be notified when someone calls you while you are already in a call. You can accept the incoming call or not. The ongoing call may be put on hold while answering the incoming call; or you may merge the calls (requires support for multiparty video conferences).

Deny: An incoming call will be rejected if you are already in a call. You will not be notified about the incoming call. However, the call will appear as a missed call in the call history list.

Conference Presentation RelayQuality

This configuration applies to video systems that are using the built-in MultiSite feature (optional) to host a multipoint video conference. When a remote user shares a presentation, the video system (codec) will transcode the presentation and send it to the other participants in the multipoint conference. The RelayQuality setting specifies whether to give priority to high frame rate or to high resolution for the presentation source.

Requires user role: ADMIN

Default value: Off

Value space: Motion/Sharpness

Motion: Gives the highest possible frame rate. Used when there is a need for higher frame rates, typically when there is a lot of motion in the picture.

Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Conference Presentation OnPlacedOnHold

Define whether or not to continue sharing a presentation after the remote site has put you on hold.

Requires user role: ADMIN

Default value: NoAction

Value space: Stop/NoAction

Stop: The video system stops the presentation sharing when the remote site puts you on hold. The presentation will not continue when the call is resumed.

NoAction: The video system will not stop the presentation sharing when put on hold. The presentation will not be shared while you are on hold, but it will continue automatically when the call is resumed.

Conference VideoBandwidth Mode

Define the conference video bandwidth mode.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The available transmit bandwidth for the video channels are distributed among the currently active channels. If there is no presentation, the main video channels will use the bandwidth of the presentation channel.

Static: The available transmit bandwidth is assigned to each video channel, even if it is not active.

Conference VideoBandwidth MainChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Default value: 5

Value space: Integer (1..10)

Set the bandwidth weight for the main channel.

Conference VideoBandwidth PresentationChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Default value: 5

Value space: Integer (1..10)

Set the bandwidth weight for the presentation channel.

FacilityService settings

FacilityService Service [1..5] Type

Up to five different facility services can be supported simultaneously. With this setting you can select what kind of services they are. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Only FacilityService Service [1] with Type Helpdesk is available on the Touch controller.

Requires user role: ADMIN

Default value: Helpdesk

Value space: Other/Concierge/Helpdesk/Emergency/Security/Catering/Transportation

Other: Select this option for services not covered by the other options.

Concierge: Select this option for concierge services.

Helpdesk: Select this option for helpdesk services.

Emergency: Select this option for emergency services.

Security: Select this option for security services.

Catering: Select this option for catering services.

Transportation: Select this option for transportation services.

FacilityService Service [1..5] Name

Define the name of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Only FacilityService Service [1] is available on the Touch controller. The name will show on the facility service call button, which appears when you tap the question mark icon in the top bar.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

The name of the facility service.

FacilityService Service [1..5] Number

Define the number (URI or phone number) of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Only FacilityService Service [1] is available on the Touch controller.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

The number (URI or phone number) of the facility service.

FacilityService Service [1..5] CallType

Define the call type for each facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Only FacilityService Service [1] is available on the Touch controller.

Requires user role: ADMIN

Default value: Video

Value space: Video/Audio

Video: Select this option for video calls.

Audio: Select this option for audio calls.

GPIO settings

GPIO Pin [1..4] Mode

The four GPIO pins are configured individually. The state can be retrieved by "xStatus GPIO Pin [1..4] State". The default pin state is High (+12 V). When activated as output, they are set to 0 V. To activate them as input, they must be pulled down to 0 V.

Requires user role: ADMIN

Default value: InputNoAction

Value space: InputNoAction/OutputManualState/OutputInCall/OutputMicrophonesMuted/OutputPresentationOn/OutputAllCallsEncrypted/OutputStandbyActive/ InputMuteMicrophones

InputNoAction: The pin state can be set, but no operation is performed.

OutputManualState: The pin state can be set by "xCommand GPIO ManualState Set PinX: <High/Low>" (to +12 V or 0 V, respectively).

OutputInCall: The pin is activated when in call, deactivated when not in call.

OutputMicrophonesMuted: The pin is activated when microphones are muted, deactivated when not muted.

OutputPresentationOn: The pin is activated when presentation is active, deactivated when presentation is not active.

OutputAllCallsEncrypted: The pin is activated when all calls are encrypted, deactivated when one or more calls are not encrypted.

OutputStandbyActive: The pin is activated when the system is in standby mode, deactivated when no longer in standby.

InputMuteMicrophones: When the pin is activated (0 V), the microphones will be muted. When deactivated (+12 V), the microphones are unmuted.

H323 settings

H323 Authentication Mode

Define the authentication mode for the H.323 profile.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

On: If an H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. Requires the H323 Authentication LoginName and H323 Authentication Password settings to be defined on both the codec and the Gatekeeper.

H323 Authentication LoginName

The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication login name.

H323 Authentication Password

The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication password.

H323 CallSetup Mode

Defines whether to use a Gatekeeper or Direct calling when establishing H.323 calls. Direct H.323 calls can be made also when H323 CallSetup Mode is set to Gatekeeper.

Requires user role: ADMIN

Default value: Gatekeeper

Value space: Direct/Gatekeeper

Direct: You can only make an H.323 call by dialing an IP address directly.

Gatekeeper: The system uses a Gatekeeper to make an H.323 call. When choosing this option, the H323 Gatekeeper Address must also be configured.

H323 Encryption KeySize

Define the minimum or maximum key size for the Diffie-Hellman key exchange method, which is used when establishing the Advanced Encryption Standard (AES) encryption key.

Requires user role: ADMIN

Default value: Max1024bit

Value space: Min1024bit/Max1024bit/Min2048bit

Min1024bit: The minimum size is 1024 bit.

Max1024bit: The maximum size is 1024 bit.

Min2048bit: The minimum size is 2048 bit.

H323 Gatekeeper Address

Define the IP address of the Gatekeeper. Requires H323 CallSetup Mode to be set to Gatekeeper.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

H323 H323Alias E164

The H.323 Alias E.164 defines the address of the system, according to the numbering plan implemented in the H.323 Gatekeeper. The E.164 alias is equivalent to a telephone number, sometimes combined with access codes.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 30)

The H.323 Alias E.164 address. Valid characters are 0-9, * and #.

H323 H323Alias ID

Define the H.323 Alias ID, which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 49)

The H.323 Alias ID. Example: "firstname.lastname@company.com", "My H.323 Alias ID"

H323 NAT Mode

The firewall traversal technology creates a secure path through the firewall barrier, and enables proper exchange of audio/video data when connected to an external video conferencing system (when the IP traffic goes through a NAT router). NOTE: NAT does not work in conjunction with gatekeepers.

Requires user role: ADMIN

Default value: Off

Value space: Auto/Off/On

Auto: The system will determine if the H323 NAT Address or the real IP address should be used in signaling. This makes it possible to place calls to endpoints on the LAN as well as endpoints on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.

Off: The system will signal the real IP address.

On: The system will signal the configured H323 NAT Address instead of its real IP address in Q.931 and H.245. The NAT server address will be shown in the startup-menu as: "My IP Address: 10.0.2.1". If the H323 NAT Address is wrong or not set, H.323 calls cannot be set up.

H323 NAT Address

Define the external/global IP address to the router with NAT support. Packets sent to the router will then be routed to the system. Note that NAT cannot be used when registered to a gatekeeper.

In the router, the following ports must be routed to the system's IP address:

- * Port 1720
- * Port 5555-6555
- * Port 2326-2487

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

H323 PortAllocation

This setting affects the H.245 port numbers used for H.323 call signaling.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

Static: When set to Static the ports are given within a static predefined range [5555-6555].

Logging settings

Logging Mode

Define the logging mode for the video system (syslog service). When disabled, the syslog service does not start, and most of the event logs are not generated. The Historical Logs and Call Logs are not affected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the system logging service.

On: Enable the system logging service.

Network settings

Network [1] DNS Domain Name

The DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is "company.com" and the name to lookup is "MyVideoSystem", this will result in the DNS lookup "MyVideoSystem.company.com".

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The DNS domain name.

Network [1] DNS Server [1..3] Address

Define the network addresses for DNS servers. Up to three addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

Network [1] IEEE8021X Mode

The system can be connected to an IEEE 802.1X LAN network, with a port-based network access control that is used to provide authenticated network access for Ethernet networks.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The 802.1X authentication is disabled (default).

On: The 802.1X authentication is enabled.

Network [1] IEEE8021X TlsVerify

Verification of the server-side certificate of an IEEE802.1x connection against the certificates in the local CA-list when TLS is used. The CA-list must be uploaded to the video system. This can be done from the web interface.

This setting takes effect only when Network [1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: When set to Off, TLS connections are allowed without verifying the server-side X.509 certificate against the local CA-list. This should typically be selected if no CA-list has been uploaded to the codec.

On: When set to On, the server-side X.509 certificate will be validated against the local CA-list for all TLS connections. Only servers with a valid certificate will be allowed.

Network [1] IEEE8021X UseClientCertificate

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: When set to Off client-side authentication is not used (only server-side).

On: When set to On the client (video system) will perform a mutual authentication TLS handshake with the server.

Network [1] IEEE8021X Identity

Define the user name for 802.1X authentication.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The user name for 802.1X authentication.

Network [1] IEEE8021X Password

Define the password for 802.1X authentication.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 32)

The password for 802.1X authentication.

Network [1] IEEE8021X AnonymousIdentity

The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The 802.1X Anonymous ID string.

Network [1] IEEE8021X Eap Md5

Define the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled (default).

Network [1] IEEE8021X Eap Ttls

Define the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled (default).

Network [1] IEEE8021X Eap Tls

Enable or disable the use of EAP-TLS (Transport Layer Security) for IEEE802.1x connections. The EAP-TLS protocol, defined in RFC 5216, is considered one of the most secure EAP standards. LAN clients are authenticated using client certificates.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled (default).

Network [1] IEEE8021X Eap Peap

Define the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled (default).

Network [1] IPStack

Select if the system should use IPv4, IPv6, or dual IP stack, on the network interface. NOTE: After changing this setting you may have to wait up to 30 seconds before it takes effect.

Requires user role: ADMIN

Default value: Dual

Value space: Dual/IPv4/IPv6

Dual: When set to Dual, the network interface can operate on both IP versions at the same time, and can have both an IPv4 and an IPv6 address at the same time.

IPv4: When set to IPv4, the system will use IPv4 on the network interface.

IPv6: When set to IPv6, the system will use IPv6 on the network interface.

Network [1] IPv4 Assignment

Define how the system will obtain its IPv4 address, subnet mask and gateway address. This setting only applies to systems on IPv4 networks.

Requires user role: ADMIN

Default value: DHCP

Value space: Static/DHCP

Static: The addresses must be configured manually using the Network IPv4 Address, Network IPv4 Gateway and Network IPv4 SubnetMask settings (static addresses).

DHCP: The system addresses are automatically assigned by the DHCP server.

Network [1] IPv4 Address

Define the static IPv4 network address for the system. Applicable only when Network IPv4 Assignment is set to Static.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

Network [1] IPv4 Gateway

Define the IPv4 network gateway address. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

Network [1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

Network [1] IPv6 Assignment

Define how the system will obtain its IPv6 address and the default gateway address. This setting only applies to systems on IPv6 networks.

Requires user role: ADMIN

Default value: Autoconf

Value space: Static/DHCPv6/Autoconf

Static: The codec and gateway IP addresses must be configured manually using the Network IPv6 Address and Network IPv6 Gateway settings. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

DHCPv6: All IPv6 addresses, including options, will be obtained from a DHCPv6 server. See RFC 3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC 4862 for a detailed description. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

Network [1] IPv6 Address

Define the static IPv6 network address for the system. Applicable only when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv6 address.

Network [1] IPv6 Gateway

Define the IPv6 network gateway address. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv6 address.

Network [1] IPv6 DHCPOptions

Retrieve a set of DHCP options, for example NTP and DNS server addresses, from a DHCPv6 server.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the retrieval of DHCP options from a DHCPv6 server.

On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

Network [1] MTU

Define the Ethernet MTU (Maximum Transmission Unit).

Requires user role: ADMIN

Default value: 1500

Value space: Integer (576..1500)

Set a value for the MTU (bytes).

Network [1] QoS Mode

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Requires user role: ADMIN

Default value: Diffserv

Value space: Off/Diffserv

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to Diffserv, the Network QoS Diffserv Audio, Network QoS Diffserv Video, Network QoS Diffserv Data, Network QoS Diffserv Signalling, Network QoS Diffserv ICMPv6 and Network QoS Diffserv NTP settings are used to prioritize packets.

Network [1] QoS Diffserv Audio

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Audio packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Audio is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the audio packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Video

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets on the presentation channel (shared content) are also in the Video packet category. The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Video is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the video packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Data

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Data packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for Data is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the data packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Signalling

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Signalling packets that are deemed critical (time-sensitive) for the real-time operation should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Signalling is CS3, which equals the decimal value 24. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the signalling packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv ICMPv6

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority ICMPv6 packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for ICMPv6 is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the ICMPv6 packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv NTP

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority NTP packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for NTP is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..63)

Set the priority of the NTP packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] RemoteAccess Allow

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the codec from SSH/Telnet/HTTP/HTTPS. Multiple IP addresses are separated by a white space.

A network mask (IP range) is specified by <ip address>/N, where N is 1-32 for IPv4, and N is 1-128 for IPv6. The /N is a common indication of a network mask where the first N bits are set. Thus 192.168.0.0/24 would match any address starting with 192.168.0, since these are the first 24 bits in the address.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address or IPv6 address.

Network [1] Speed

Define the Ethernet link speed.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/10half/10full/100half/100full/1000full

Auto: Autonegotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

1000full: Force link to 1 Gbps full-duplex.

Network [1] TrafficControl Mode

Define the network traffic control mode to decide how to control the video packets transmission speed.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Transmit video packets at link speed.

On: Transmit video packets at maximum 20 Mbps. Can be used to smooth out bursts in the outgoing network traffic.

Network [1] VLAN Voice Mode

Define the VLAN voice mode. The VLAN Voice Mode will be set to Auto automatically if you have Cisco UCM (Cisco Unified Communications Manager) as provisioning infrastructure. Note that Auto mode will NOT work if the NetworkServices CDP Mode setting is Off.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Manual/Off

Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled.

Manual: The VLAN ID is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.

Off: VLAN is not enabled.

Network [1] VLAN Voice VlanId

Define the VLAN voice ID. This setting will only take effect if Network VLAN Voice Mode is set to Manual.

Requires user role: ADMIN

Default value: 1

Value space: Integer (1..4094)

Set the VLAN voice ID.

NetworkServices settings

NetworkServices CDP Mode

Enable or disable the CDP (Cisco Discovery Protocol) daemon. Enabling CDP will make the endpoint report certain statistics and device identifiers to a CDP-enabled switch. If CDP is disabled, the Network VLAN Voice Mode: Auto setting will not work.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

NetworkServices H323 Mode

Define whether the system should be able to place and receive H.323 calls or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the possibility to place and receive H.323 calls.

On: Enable the possibility to place and receive H.323 calls (default).

NetworkServices HTTP Mode

Define whether or not to allow access to the video system using the HTTP or HTTPS (HTTP Secure) protocols. Note that the video system's web interface use HTTP or HTTPS. If this setting is switched Off, you cannot use the web interface.

If you need extra security (encryption and decryption of requests, and pages that are returned by the web server), allow only HTTPS.

Requires user role: ADMIN

Default value: HTTP+HTTPS

Value space: Off/HTTP+HTTPS/HTTPS

Off: Access to the video system not allowed via HTTP or HTTPS.

HTTP+HTTPS: Access to the video system allowed via both HTTP and HTTPS.

HTTPS: Access to the video system allowed via HTTPS, but not via HTTP.

NetworkServices HTTPS VerifyServerCertificate

When the video system connects to an external HTTPS server (like a phone book server or an external manager), this server will present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify server certificates.

On: Requires the system to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS VerifyClientCertificate

When the video system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify client certificates.

On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS OCSP Mode

Define the support for OCSP (Online Certificate Status Protocol) responder services. The OCSP feature allows users to enable OCSP instead of certificate revocation lists (CRLs) to check the certificate status.

For any outgoing HTTPS connection, the OCSP responder is queried of the status. If the corresponding certificate has been revoked, then the HTTPS connection will not be used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable OCSP support.

On: Enable OCSP support.

NetworkServices HTTPS OCSP URL

Define the URL of the OCSP responder (server) that will be used to check the certificate status.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid URL.

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the system's time and date to a reference time server. The time server will be queried regularly for time updates.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Manual/Off

Auto: The system will use an NTP server for time reference. As default, the server address will be obtained from the network's DHCP server. If a DHCP server is not used, or if the DHCP server does not provide an NTP server address, the NTP server address that is specified in the NetworkServices NTP Server [n] Address setting will be used.

Manual: The system will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The system will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

NetworkServices NTP Server [1..3] Address

The address of the NTP server that will be used when NetworkServices NTP Mode is set to Manual, and when NetworkServices NTP Mode is set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN

Default value: 0.tandberg.pool.ntp.org

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SIP Mode

Define whether the system should be able to place and receive SIP calls or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the possibility to place and receive SIP calls.

On: Enable the possibility to place and receive SIP calls (default).

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Requires user role: ADMIN

Default value: ReadOnly

Value space: Off/ReadOnly/ReadWrite

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

ReadWrite: Enable the SNMP network service for both queries and commands.

NetworkServices SNMP Host [1..3] Address

Define the address of up to three SNMP Managers.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), for example about system location and system contact. SNMP traps are not supported.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SNMP CommunityName

Define the name of the Network Services SNMP Community. SNMP Community names are used to authenticate SNMP requests. SNMP requests must have a password (case sensitive) in order to receive a response from the SNMP Agent in the codec. The default password is "public". If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE: The SNMP Community password is case sensitive.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The SNMP community name.

NetworkServices SNMP SystemContact

Define the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The name of the SNMP system contact.

NetworkServices SNMP SystemLocation

Define the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The name of the SNMP system location.

NetworkServices SSH Mode

SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the codec.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH public key is not allowed.

On: The SSH public key is allowed.

NetworkServices Telnet Mode

Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The Telnet protocol is disabled. This is the factory setting.

On: The Telnet protocol is enabled.

NetworkServices UPnP Mode

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video system has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video system. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting.

When UPnP is enabled, the video system advertises its presence on the network. The advertisement permits a Touch controller to discover video systems automatically, and you do not need to manually enter the video system's IP address in order to pair the Touch controller.

Requires user role: ADMIN

Default value: On

Value space: <Off/On>

Off: UPnP is disabled. The video system does not advertise its presence, and you have to enter the video system's IP address manually in order to pair a Touch controller to the video system.

On: UPnP is enabled. The video system advertises its presence until the timeout period expires.

NetworkServices UPnP Timeout

Define for how many seconds UPnP shall stay enabled after the video system is switched on or restarted. The NetworkServices UPnP Mode setting must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: 600

Value space: <0..3600>

Range: Select a value between 0 and 3600 seconds.

NetworkServices WelcomeText

Choose which information the user should see when logging on to the codec through Telnet/SSH.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The welcome text is: Login successful

On: The welcome text is: Welcome to <system name>; Software version; Software release date; Login successful.

NetworkServices XMLAPI Mode

Enable or disable the video system's XML API. For security reasons this may be disabled. Disabling the XML API will limit the remote manageability with for example TMS, which no longer will be able to connect to the video system.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The XML API is disabled.

On: The XML API is enabled (default).

Peripherals settings

Peripherals Pairing CiscoTouchPanels RemotePairing

In order to use Cisco Touch 10 (touch panel) as user interface for the video system, Touch 10 must be either directly connected to the video system or paired to the video system via LAN. The latter is referred to as remote pairing.

Remote pairing is allowed by default; you must switch this setting Off if you want to prevent remote pairing.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Remote pairing of Touch 10 is not allowed.

On: Remote pairing of Touch 10 is allowed.

Peripherals Pairing Ultrasound Volume Mode

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The video system adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Peripherals Pairing Ultrasound Volume MaxLevel setting.

Static: Use only if advised by Cisco.

Peripherals Pairing Ultrasound Volume MaxLevel

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message. Refer to the Peripherals Pairing Ultrasound Volume Mode setting.

Requires user role: ADMIN

Default value: 70

Value space: Integer (0..90)

Select a value between 0 and 90. If set to 0, the ultrasound is switched off.

Peripherals Profile TouchPanels

Define the number of touch panels that are expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected touch panels does not match this setting, the diagnostics service will report it as an inconsistency. Note that only one Cisco Touch controller is supported in this version.

Requires user role: ADMIN

Default value: NotSet

Value space: NotSet/Minimum1/0/1/2/3/4/5

NotSet: No touch panel check is performed.

Minimum1: At least one touch panel should be connected to the video system.

0-5: Select the number of Touch controllers that are expected to be connected to the video system.

Phonebook settings

Phonebook Server [1] ID

Define a name for the external phone book.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The name for the external phone book.

Phonebook Server [1] Type

Select the phonebook server type.

Requires user role: ADMIN

Default value: Off

Value space: Off/VCS/TMS/CUCM

Off: Do not use a phonebook.

VCS: The phonebook is located on the Cisco TelePresence Video Communication Server.

TMS: The phonebook is located on the Cisco TelePresence Management Suite server.

CUCM: The phonebook is located on the Cisco Unified Communications Manager.

Phonebook Server [1] URL

Define the address (URL) to the external phone book server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid address (URL) to the phone book server.

Provisioning settings

Provisioning Connectivity

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN

Default value: Auto

Value space: Internal/External/Auto

Internal: Request internal configuration.

External: Request external configuration.

Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the "e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

Provisioning Mode

It is possible to configure a video system using a provisioning system (external manager). This allows video conferencing network administrators to manage many video systems simultaneously. With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/representative for more information.

Requires user role: ADMIN

Default value: Auto

Value space: Off/Auto/TMS/VCS/CUCM/Edge

Off: The video system is not configured by a provisioning system.

Auto: Automatically select the provisioning server.

TMS: Push configurations to the video system from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the video system from VCS (Cisco TelePresence Video Communication Server).

CUCM: Push configurations to the video system from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the video system from CUCM (Cisco Unified Communications Manager). The system connects to CUCM via the Collaboration Edge infrastructure.

Provisioning LoginName

This is the username part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 80)

A valid username.

Provisioning Password

This is the password part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid password.

Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

Requires user role: ADMIN

Default value: POST

Value space: GET/POST

GET: Select GET when the provisioning server supports GET.

POST: Select POST when the provisioning server supports POST.

Provisioning ExternalManager Address

Define the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the system will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.

When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager AlternateAddress

Only applicable when the endpoint is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Define the address of the alternate CUCM. If the main CUCM is not available, the endpoint will be provisioned by the alternate CUCM. When the main CUCM is available again, the endpoint will be provisioned by this CUCM.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager Protocol

Define whether to use the HTTP (unsecure communication) or HTTPS (secure communication) protocol when sending requests to the external manager / provisioning system.

The chosen protocol must be enabled in the NetworkServices HTTP Mode setting.

Requires user role: ADMIN

Default value: HTTP

Value space: HTTPS/HTTP

HTTPS: Send requests via HTTPS.

HTTP: Send requests via HTTP.

Provisioning ExternalManager Path

Define the Path to the external manager / provisioning system. This setting is required when several management services reside on the same server, i.e. share the same External Manager address.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid path to the external manager or provisioning system.

Provisioning ExternalManager Domain

Define the SIP domain for the VCS provisioning server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid domain name.

Proximity settings

Proximity Mode

Determine whether the video system will emit ultrasound pairing messages or not.

When the video system emits ultrasound, Proximity clients can detect that they are close to the video system. In order to use a client, at least one of the Proximity services must be enabled (refer to the Proximity Services settings). In general, Cisco recommends enabling all the Proximity services.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The video system does not emit ultrasound, and Proximity services cannot be used.

On: The video system emits ultrasound, and Proximity clients can detect that they are close to the video system. Enabled Proximity services can be used.

Proximity Services CallControl

Enable or disable basic call control features on Proximity clients. When this setting is enabled, you are able to control a call using a Proximity client (for example dial, mute, adjust volume and hang up). This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Call control from a Proximity client is enabled.

Disabled: Call control from a Proximity client is disabled.

Proximity Services ContentShare FromClients

Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the video system, e.g. share your laptop screen. This service is supported by laptops (OS X and Windows). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Content sharing from a Proximity client is enabled.

Disabled: Content sharing from a Proximity client is disabled.

Proximity Services ContentShare ToClients

Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the video system. You can zoom in on details, view previous content and take snapshots. This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Content sharing to a Proximity client is enabled.

Disabled: Content sharing to a Proximity client is disabled.

RTP settings

RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

NOTE: Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 2326

Value space: Integer (1024..65438)

Set the first port in the range of RTP ports.

RTP Ports Range Stop

Define the last port in the range of RTP ports.

As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

NOTE: Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 2486

Value space: Integer (1120..65535)

Set the last port in the range of RTP ports.

Security settings

Security Audit Logging Mode

Define where to record or transmit the audit logs. The audit logs are sent to a syslog server. When using the External/ExternalSecure modes and setting the port assignment to manual in the Security Audit Server PortAssignment setting, you must also enter the address and port number for the audit server in the Security Audit Server Address and Security Audit Server Port settings.

Requires user role: AUDIT

Default value: Off

Value space: Off/Internal/External/ExternalSecure

Off: No audit logging is performed.

Internal: The system records the audit logs to internal logs, and rotates logs when they are full.

External: The system sends the audit logs to an external syslog server. The syslog server must support UDP.

ExternalSecure: The system sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the codec using the web interface. The `common_name` parameter of a certificate in the CA list must match the IP address of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

Security Audit OnError Action

Define what happens when the connection to the syslog server is lost. This setting is only relevant when Security Audit Logging Mode is set to ExternalSecure.

Requires user role: AUDIT

Default value: Ignore

Value space: Halt/Ignore

Halt: If a halt condition is detected the system codec is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the syslog server. Halt conditions are: A network breach (no physical link), no syslog server running (or incorrect address or port to the syslog server), TLS authentication failed (if in use), local backup (re-spooling) log full.

Ignore: The system will continue its normal operation, and rotate internal logs when full. When the connection is restored it will again send its audit logs to the syslog server.

Security Audit Server Address

The audit logs are sent to a syslog server. Define the IP address of the syslog server. Only valid IPv4 or IPv6 address formats are accepted. Host names are not supported. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

Requires user role: AUDIT

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address

Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the system shall send its audit logs to. This setting is only relevant when Security Audit Server PortAssignment is set to Manual.

Requires user role: AUDIT

Default value: 514

Value space: Integer (0..65535)

Set the audit server port.

Security Audit Server PortAssignment

The audit logs are sent to a syslog server. You can define how the port number of the external syslog server will be assigned. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure. To see which port number is used you can check the Security Audit Server Port status. Navigate to Configuration > System status on the web interface or; if on a command line interface, run the command `xStatus Security Audit Server Port`.

Requires user role: AUDIT

Default value: Auto

Value space: Auto/Manual

Auto: Will use UDP port number 514 when the Security Audit Logging Mode is set to External. Will use TCP port number 6514 when the Security Audit Logging Mode is set to ExternalSecure.

Manual: Will use the port value defined in the Security Audit Server Port setting.

Security Session InactivityTimeout

Define how long the system will accept inactivity from the user before he is automatically logged out.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10000)

Set the inactivity timeout (seconds); or select 0 when inactivity should not enforce automatic logout.

Security Session ShowLastLogon

When logging in to the system using SSH or Telnet you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

On: Show information about the last session.

Off: Do not show information about the last session.

SerialPort settings

SerialPort Mode

Enable/disable the serial port (COM port).

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the serial port.

On: Enable the serial port.

SerialPort BaudRate

Define the baud rate (data transmission rate, bits per second) for the serial port. The default value is 115200.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

Requires user role: ADMIN

Default value: 115200

Value space: 9600/19200/38400/57600/115200

Set a baud rate from the baud rates listed (bps).

SerialPort LoginRequired

Define if login shall be required when connecting to the serial port.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The user can access the codec via the serial port without any login.

On: Login is required when connecting to the codec via the serial port.

SIP settings

SIP ANAT

ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable ANAT.

On: Enable ANAT.

SIP Authentication UserName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid username.

SIP Authentication Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

SIP DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Default value: Auto

Value space: TCP/UDP/Tls/Auto

TCP: The system will always use TCP as the default transport method.

UDP: The system will always use UDP as the default transport method.

Tls: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the video system. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

SIP DisplayName

When configured the incoming call will report the display name instead of the SIP URI.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The name to be displayed instead of the SIP URI.

SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the endpoints can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the endpoints. NOTE: ICE is not supported when registered to CUCM (Cisco Unified Communication Manager).

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

Auto: When set to Auto, ICE will be enabled if a turn server is provided, otherwise ICE will be disabled.

Off: Set to Off to disable ICE.

On: Set to On to enable ICE.

SIP Ice DefaultCandidate

This is the default IP address that the endpoint will receive media on until ICE has reached a conclusion about which media route to use (up to the first 5 seconds of a call).

Requires user role: ADMIN

Default value: Host

Value space: Host/Rflx/Relay

Host: The endpoint will receive media on its own IP address.

Rflx: The endpoint will receive media on its public IP address as seen by the TURN server.

Relay: The endpoint will receive media on the IP address and port allocated on the TURN server, and is used as a fallback until ICE has concluded.

SIP Line

When registered to a Cisco Unified Communications Manager (CUCM) the endpoint may be part of a shared line. This means that several devices share the same directory number. The different devices sharing the same number receive status from the other appearances on the line as defined in RFC 4235.

Note that shared lines are set up by CUCM, not by the endpoint. Therefore do not change this setting manually; CUCM pushes this information to the endpoint when required.

Requires user role: ADMIN

Default value: Private

Value space: Private/Shared

Shared: The system is part of a shared line and is therefore sharing its directory number with other devices.

Private: This system is not part of a shared line (default).

SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the endpoint will only be reachable through the SIP registrar (CUCM or VCS). It is recommended to leave this setting at its default value.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Listening for incoming connections on the SIP TCP/UDP ports is turned off.

On: Listening for incoming connections on the SIP TCP/UDP ports is turned on.

SIP Mailbox

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255>)

A valid number or address. Leave the string empty if you do not have a voice mailbox.

SIP PreferredIPMedia

Define the preferred IP version for sending and receiving media (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for media is IPv4.

IPv6: The preferred IP version for media is IPv6.

SIP PreferredIPSignaling

Define the preferred IP version for signaling (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version. It also determines the priority of the A/AAAA lookups in DNS, so that the preferred IP version is used for registration.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

SIP Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

SIP TlsVerify

For TLS connections a SIP CA-list can be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.

On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the system will test if port allocation is possible.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Set to Off to disable discovery mode.

On: When set to On, the system will search for available Turn servers in DNS, and before making calls the system will test if port allocation is possible.

SIP Turn BandwidthProbe

Not applicable in this version.

SIP Turn DropRflx

DropRflx will make the endpoint force media through the Turn relay, unless the remote endpoint is on the same network.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable DropRflx.

On: The system will force media through the Turn relay when the remote endpoint is on another network.

SIP Turn Server

Define the address of the TURN (Traversal Using Relay NAT) server. It is used as a media relay fallback and it is also used to discover the endpoint's own public IP address.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The preferred format is DNS SRV record (e.g. `_turn._udp.<domain>`), or it can be a valid IPv4 or IPv6 address.

SIP Turn UserName

Define the user name needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid user name.

SIP Turn Password

Define the password needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

SIP Type

Enables SIP extensions and special behavior for a vendor or provider.

Requires user role: ADMIN

Default value: Standard

Value space: Standard/Cisco

Standard: Use this when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)

Cisco: Use this when registering to Cisco Unified Communication Manager.

SIP URI

The SIP URI (Uniform Resource Identifier) is the address that is used to identify the video system. The URI is registered and used by the SIP services to route inbound calls to the system. The SIP URI syntax is defined in RFC 3261.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

An address (URI) that is compliant with the SIP URI syntax.

Standby settings

Standby Control

Define whether the system should go into standby mode or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The system will not enter standby mode.

On: The system will enter standby mode when the Standby Delay has timed out.
Requires the Standby Delay to be set to an appropriate value.

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. Requires the Standby Control to be enabled.

Requires user role: ADMIN

Default value: 10

Value space: Integer (1..480)

Set the standby delay (minutes).

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN

Default value: DefaultCameraPosition

Value space: None/RestoreCameraPosition/DefaultCameraPosition

None: No action.

RestoreCameraPosition: When the video system restarts, the camera returns to the position that it had before the restart.

DefaultCameraPosition: When the video system restarts, the camera moves to the factory default position.

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN

Default value: PrivacyPosition

Value space: None/PrivacyPosition

None: No action.

PrivacyPosition: When the video system enters standby, the camera turns to a sideways position for privacy.

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN

Default value: RestoreCameraPosition

Value space: None/RestoreCameraPosition/DefaultCameraPosition

None: No action.

RestoreCameraPosition: When the video system leaves standby, the camera returns to the position that it had before entering standby.

DefaultCameraPosition: When the video system leaves standby, the camera moves to the factory default position.

SystemUnit settings

SystemUnit Name

Define the system name. The system name will be sent as the hostname in a DHCP request and when the codec is acting as an SNMP Agent.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

Define the system name.

Time settings

Time TimeFormat

Define the time format.

Requires user role: USER

Default value: 24H

Value space: 24H/12H

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours (AM/PM).

Time DateFormat

Define the date format.

Requires user role: USER

Default value: DD_MM_YY

Value space: DD_MM_YY/MM_DD_YY/YY_MM_DD

DD_MM_YY: The date January 30th 2010 will be displayed: 30.01.10

MM_DD_YY: The date January 30th 2010 will be displayed: 01.30.10

YY_MM_DD: The date January 30th 2010 will be displayed: 10.01.30

Time Zone

Define the time zone for the geographical location of the video system. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: USER

Default value: Etc/UTC

Value space: Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/EL_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal,

America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Porto_Velho, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/

GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu>

Select a time zone from the list.

UserInterface settings

UserInterface ContactInfo Type

Choose which type of contact information to show in the status field in the upper left corner of the display and Touch controller.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/None/IPv4/IPv6/H323Id/H320Number/E164Alias/SipUri/SystemName/DisplayName

Auto: Show the address which another system should dial to reach this video system. The address depends on the default call protocol and system registration.

None: Do not show any contact information.

IPv4: Show the system's IPv4 address.

IPv6: Show the system's IPv6 address.

H323Id: Show the system's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the system's H.320 number as contact information (only applicable if connected to Cisco TelePresence ISDN Link).

E164Alias: Show the system's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

SipUri: Show the system's SIP URI (refer to the SIP URI setting).

SystemName: Show the system's name (refer to the SystemUnit Name setting).

DisplayName: Show the system's display name (refer to the SIP DisplayName setting).

UserInterface KeyTones Mode

You can configure the system to make a keyboard click sound effect (key tone) when typing text or numbers on the Touch controller.

Requires user role: USER

Default value: On

Value space: Off/On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

UserInterface Language

Select the language to be used in menus and messages on the screen and Touch controller. The default language is English.

Requires user role: USER

Default value: English

Value space: English/ChineseSimplified/ChineseTraditional/Catalan/Czech/Danish/Dutch/Finnish/French/German/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/Swedish/Turkish/Arabic/Hebrew

Select a language from the list.

UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator (a padlock) is shown on screen. The icon for encrypted calls is a locked padlock, and the icon for non-encrypted calls is a crossed out locked padlock.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/AlwaysOn/AlwaysOff

Auto: If the call is encrypted, a "Call is encrypted" notification is shown for 5 seconds, while the encryption indicator icon is shown for the duration of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. Also the encryption indicator icon disappears from screen after 5 seconds.

AlwaysOn: The encryption indicator is displayed on screen during the entire call.

AlwaysOff: The encryption indicator is never displayed on screen.

UserInterface OSD Output

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/1/2/3

Auto: The system detects when a monitor is connected to a video output, and sends the on-screen information and indicators to the first monitor you connect. If you have a multi-monitor setup, and all monitors are connected before switching on the system, the on-screen information and indicators are sent to the video output with the lowest number, starting with Output Connector 1 (HDMI 1).

Range 1-3: The system sends the on-screen information and indicators to the specified output. Choose n to send the on-screen information and indicators to the system's Output Connector n.

UserInterface Wallpaper

Select a background image (wallpaper) for the video screen when idle.

You may upload a custom wallpaper to the video system using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 2 MByte.

Requires user role: USER

Default value: None

Value space: None/Custom

None: There is no background image on the screen.

Custom: Use the custom wallpaper as background image on the screen. If no custom wallpaper is uploaded to the system, the setting will revert to the default value.

UserInterface UserPreferences

Some user preferences (ringtone, volume, language, date and time, etc) can be made available from the Settings menu, or from the Settings > Administrator menu on the Touch controller. Accessing the Administrator menus requires that the user has admin privileges.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The user preferences are available from the Settings > Administrator menu on the Touch controller, for users with admin privileges.

On: The user preferences are available from the Settings menu on the Touch controller.

Video settings

Video ActiveSpeaker DefaultPIPPosition

Define the position on screen of the active speaker picture-in-picture (PiP). The setting only takes effect when using a video layout where the active speaker is a PiP, i.e. the Overlay layout, or possibly a Custom layout (refer to the Video DefaultLayoutFamily Local setting). The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the active speaker PiP will be kept unchanged when leaving a call.

UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.

UpperCenter: The active speaker PiP will appear in the upper center position.

UpperRight: The active speaker PiP will appear in the upper right corner of the screen.

CenterLeft: The active speaker PiP will appear in the center left position.

CenterRight: The active speaker PiP will appear in the center right position.

LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.

LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

Video DefaultLayoutFamily Local

Select which video layout family to use locally.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single>

Auto: The default layout family, as given in the layout database provided by the system, will be used as the local layout.

Equal: The Equal layout family will be used as the local layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the local layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the local layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video DefaultLayoutFamily Remote

Select which video layout family to be used for the remote participants.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single

Auto: The default layout family, as given by the local layout database, will be used as the remote layout.

Equal: The Equal layout family will be used as the remote layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the remote layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the remote layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PIP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video DefaultMainSource

Define which video input source shall be used as the main video source.

Requires user role: USER

Default value: 1

Value space: 1/2/3/4

Set the source to be used as the main video source.

Video Input Connector [1..5] CameraControl Mode

Define whether the camera that is connected to this video input connector can be controlled or not.

Note that camera control is not available for Connector 5 (S-video/Composite).

Requires user role: ADMIN

Default value: Connector 1, 2, 3: On Connector 4, 5: Off

Value space: Connector 1, 2, 3, 4: Off/On Connector 5: Off

Off: Disable camera control.

On: Enable camera control.

Video Input Connector [1..5] CameraControl CameraId

The camera ID is a unique identifier of the cameras that are connected to the video input. Use the xStatus Camera API command to see the IDs of the different cameras.

Requires user role: ADMIN

Default value: Connector n: n Connector 5: 1

Value space: Connector 1, 2, 3, 4: 1/2/3/4/5/6/7 Connector 5: 1

Select the ID of the camera.

Video Input Connector [4] DviType

The official DVI standard supports both digital and analog signals. In most cases the default AutoDetect setting can detect whether the signal is analog RGB or digital. However, in some rare cases when DVI-I cables are used (these cables can carry both the analog and digital signals) the auto detection fails. This setting makes it possible to override the AutoDetect and select the correct DVI video input.

Requires user role: ADMIN

Default value: AutoDetect

Value space: AutoDetect/Digital/AnalogRGB/AnalogYPbPr

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.

Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Video Input Connector [5] SignalType

Connector 5 can be used for either S-Video or Composite video input format. Use this setting to configure which video format the BNC connector(s) are used for.

Requires user role: ADMIN

Default value: Composite

Value space: Composite/YC

Composite: Connector 5 is configured for composite video input. Only the BNC connector that is labeled "Y" is used.

YC: Connector 5 is configured for S-Video input. Both BNC connectors ("Y" and "C") are used.

Video Input Connector [1..5] InputSourceType

Select which type of input source is connected to the video input.

Requires user role: ADMIN

Default value: Connector 1 and 2: camera Connector 3 and 4: PC Connector 5: other

Value space: camera/PC/mediaplayer/document_camera/whiteboard/other

camera: Use this when a camera is connected to the video input.

PC: Use this when a computer is connected to the video input.

mediaplayer: Use this when a media player is connected to the video input.

document_camera: Use this when a document camera is connected to the video input.

whiteboard: Use this when a whiteboard camera is connected to the video input.

other: Use this when the other options do not match.

Video Input Connector [1..5] Name

Define a name for the video input connector.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

Name for the video input connector.

Video Input Connector [1..5] Quality

When encoding and transmitting video there is a trade-off between high resolution and high frame rate. For some video sources it is more important to transmit high frame rate than high resolution and vice versa. This setting specifies whether to give priority to high frame rate or to high resolution.

Requires user role: ADMIN

Default value: Connector 1, 2, 5: Motion Connector 3, 4: Sharpness

Value space: Motion/Sharpness

Motion: Gives the highest possible frame rate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Video Input Connector [1..5] OptimalDefinition Profile

This setting will only take effect if the corresponding Video Input Connector [n] Quality setting is set to Motion.

The optimal definition profile reflects the lighting conditions in the video conferencing room and the quality of the camera. The better lighting conditions and the better quality of the camera, the higher the profile. In good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate. Generally, the Normal or Medium profiles are recommended. However, when the lighting conditions are very good, the High profile can be set in order to increase the resolution for a given call rate.

Some typical resolutions used for different optimal definition profiles, call rates and transmit frame rates are shown in the table below. The resolution must be supported by both the calling and called systems. Use the Video Input Connector [n] OptimalDefinition Threshold60fps setting to decide when to use the 60 fps frame rate.

Typical resolutions used for different optimal definition profiles, call rates and frame rates								
	Frame rate	Optimal Definition Profile	Call rate					
			768 kbps	1152 kbps	1472 kbps	2560 kbps	4 Mbps*	6 Mbps*
H.265 (only in SIP calls)	30 fps	Normal	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		Medium	1280×720	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080
		High	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080	1920×1080
	60 fps	Normal	768×448	1024×576	1280×720	1280×720	1280×720	1280×720
		Medium	1024×576	1280×720	1280×720	1280×720	1280×720	1280×720
		High	1280×720	1280×720	1280×720	1280×720	1280×720	1280×720
H.264	30 fps	Normal	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		Medium	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
		High	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
	60 fps	Normal	640×360	768×448	1024×576	1280×720	1280×720	1920×1080
		Medium	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
		High	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

* H.265 is preferred over H.264, and the maximum bit rate for H.265 is 3 Mbps. When the user sets a higher bit rate, the codec will still use H.265 at 3 Mbps as long as all codecs involved supports H.265.

Requires user role: ADMIN

Default value: Medium

Value space: Normal/Medium/High

Normal: Use this profile for a normally to poorly lit environment. Resolutions will be set rather conservative.

Medium: Requires good and stable lighting conditions and a good quality video input. For some call rates this leads to higher resolution.

High: Requires nearly optimal video conferencing lighting conditions and a good quality video input in order to achieve a good overall experience. Rather high resolutions will be used.

Video Input Connector [1..5] OptimalDefinition Threshold60fps

For each video input, this setting tells the system the lowest resolution where it should transmit 60fps. So for all resolutions lower than this, the maximum transmitted frame rate would be 30fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Requires user role: ADMIN

Default value: 1280_720

Value space: 512_288/768_448/1024_576/1280_720/1920_1080/Never

512_288: Set the threshold to 512x288.

768_448: Set the threshold to 768x448.

1024_576: Set the threshold to 1024x576.

1280_720: Set the threshold to 1280x720.

1920_1080: Set the threshold to 1920x1080.

Never: Do not set a threshold for transmitting 60fps.

Video Input Connector [1..4] PresentationSelection

Define how the video system will behave when you connect a presentation source to the video input. In general, any input source can be used as a presentation source; normally, the main camera will not be used as a presentation source.

If the video system is in standby mode, it will wake up when you connect a presentation source. Note that sharing the presentation with the far end always requires additional action (press Share on the user interface).

Requires user role: ADMIN

Default value: Connector 1, 2: Manual Connector 3, 4: OnConnect

Value space: Manual/OnConnect

Manual: In manual mode, the contents of the video input will not be presented on the screen until you choose it from the user interface.

OnConnect: When in on-connect mode, the content on the video input will be presented on screen when a cable is connected. Otherwise, the behavior is the same as in manual mode.

Video Input Connector [1..4] RGBQuantizationRange

The devices connected to the video input should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any source.

Requires user role: ADMIN

Default value: Connector 1, 2, 3: Auto Connector 4: Full

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on video format according to CEA-861-E. CE video formats will use limited quantization range levels. IT video formats will use full quantization range levels.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Input Connector [1..5] Visibility

Define the visibility of the video input connector in the menus on the user interface.

Requires user role: ADMIN

Default value: Connector 1, 2, 3: IfSignal Connector 4: Always Connector 5: Never

Value space: Never/Always/IfSignal

Never: When the input source is not expected to be used as a presentation source, set to Never.

Always: When set to Always, the menu selection for the video input connector will always be visible on the graphical user interface.

IfSignal: When set to IfSignal, the menu selection for the video input connector will only be visible when something is connected to the video input.

Video Monitors

A role is assigned to each monitor using the Video Output Connector [n] MonitorRole setting. The monitor role decides which layout (call participants and presentation) will appear on the monitor that is connected to this output. Monitors with the same monitor role will get the same layout; monitors with different monitor roles will have different layouts.

The monitor layout mode that is set in the Video Monitors setting should reflect the number of different layouts you want in your room setup. Note that some monitors can be reserved for presentations.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Single/Dual/DualPresentationOnly/TriplePresentationOnly/Triple

Auto: The number of monitors connected to the codec is automatically detected, and the layout is distributed on the monitors according to the MonitorRole settings.

Single: The same layout is shown on all monitors.

Dual: The layout is distributed on monitors with monitor role First and Second. If a presentation is part of the layout, all participants in the call are shown on monitors with monitor role First, and the presentation is shown on monitors with monitor role Second.

DualPresentationOnly: All participants in the call are shown on monitors with monitor role First. If a presentation is part of the layout, the presentation is shown on monitors with monitor role Second.

Triple: The layout is distributed on monitors with monitor role First, Second and Third. If a presentation is part of the layout, all participants in the call are shown on monitors with monitor role First and Second, and the presentation is shown on the monitor with monitor role Third.

TriplePresentationOnly: All participants in the call are distributed on monitors with monitor role First and Second. If a presentation is part of the layout, the presentation is shown on the monitor with monitor role Third.

Video Output Connector [1..2] CEC Mode

This video output (HDMI) supports Consumer Electronics Control (CEC). When this setting is On (default is Off), the system will use CEC to set the monitor in standby when the system itself enters standby. Likewise the system will wake up the monitor when the system itself wakes up from standby. For this to happen, the monitor that is connected to the output must be CEC compatible and CEC must be configured on the monitor.

Note that the different manufacturers uses different marketing names for CEC, for example Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable CEC control

On: Enable CEC control

Video Output Connector [1..3] Location HorizontalOffset

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have three displays side by side, with the left and right displays at equal distance from center. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display, and HorizontalOffset = 1 for the right display.

Example: You have two displays, one in center and one below. Then the following settings will apply: VerticalOffset = 0 for the center display, Vertical Offset = -1 for the lower display.

The default values for the different outputs are:

Video Output Connector [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output Connector [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector [3] Location: HorizontalOffset = 1, VerticalOffset = 0

Requires user role: ADMIN

Default value: Connector [1]: -1 Connector [2]: 0 Connector [3]: 1

Value space: Integer (-100..100)

Range: The value must be between -100 and 100.

Video Output Connector [1..3] Location VerticalOffset

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have three displays side by side, with the left and right displays at equal distance from center. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display, and HorizontalOffset = 1 for the right display.

Example: You have two displays, one in center and one below. Then the following settings will apply: VerticalOffset = 0 for the center display, Vertical Offset = -1 for the lower display.

The default values for the different outputs are:

Video Output Connector [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output Connector [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Connector [3] Location: HorizontalOffset = 1, VerticalOffset = 0

Requires user role: ADMIN

Default value: 0

Value space: Integer (-100..100)

Range: The value must be between -100 and 100.

Video Output Connector [1..3] MonitorRole

The monitor role describes which video streams will be shown on the monitor connected to this video output connector. Together the Video Monitors setting and the MonitorRole settings for all outputs define which layout (video streams) will be shown on each monitor.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/First/Second/PresentationOnly/Third/Recorder

Auto: The system will detect when a monitor is connected, and a monitor role (First, Second, Third) that corresponds with the Video Monitors setting will be assigned automatically.

First/Second/Third: Define the role of the monitor in a multi-monitor setup. In a single-monitor setup, there is no difference between First, Second and Third.

PresentationOnly: Show presentation video stream if active, and nothing else. Monitors/outputs with this monitor role are disregarded by the Video Monitors setting.

Recorder: Show all participants, including the local main video (self-view). If active, also show the presentation. Monitors/outputs with this monitor role are disregarded by the Video Monitors setting.

Video Output Connector [1..3] Resolution

Define the resolution and refresh rate for the connected screen.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/1280_720_50/1280_720_60/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

1280_720_50: The resolution is 1280 x 720, and the refresh rate is 50 Hz.

1280_720_60: The resolution is 1280 x 720, and the refresh rate is 60 Hz.

1920_1080_50: The resolution is 1920 x 1080, and the refresh rate is 50 Hz.

1920_1080_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

1920_1200_50: The resolution is 1920 x 1200, and the refresh rate is 50 Hz.

1920_1200_60: The resolution is 1920 x 1200, and the refresh rate is 60 Hz.

Video Output Connector [1..3] RGBQuantizationRange

Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any display. The default value is set to Full because most HDMI displays expects full quantization range.

Requires user role: ADMIN

Default value: Full

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe. If no AVI infoframe is available, RGB quantization range is selected based on video format according to CEA-861-E.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Presentation DefaultPIPPosition

Define the position on screen of the presentation picture-in-picture (PiP). The setting only takes effect when the presentation is explicitly minimized to a PiP, for example using the Touch controller. The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the presentation PiP will be kept unchanged when leaving a call.

UpperLeft: The presentation PiP will appear in the upper left corner of the screen.

UpperCenter: The presentation PiP will appear in the upper center position.

UpperRight: The presentation PiP will appear in the upper right corner of the screen.

CenterLeft: The presentation PiP will appear in the center left position.

CenterRight: The presentation PiP will appear in the center right position.

LowerLeft: The presentation PiP will appear in the lower left corner of the screen.

LowerRight: The presentation PiP will appear in the lower right corner of the screen.

Video Presentation DefaultSource

Define which video input source to use as a default presentation source. This setting may be used by the API and 3rd party user interfaces, but is not relevant when using Touch 10 or the TRC6 remote control.

Requires user role: USER

Default value: 3

Value space: 1/2/3/4

The video input source to use as default presentation source.

Video Selfview Default Mode

Define if the main video source (self-view) shall be displayed on screen after a call. The position and size of the self-view window is determined by the Video Selfview Default PIPPosition and the Video Selfview Default FullscreenMode settings respectively.

Requires user role: ADMIN

Default value: Current

Value space: Off/Current/On

Off: self-view is switched off when leaving a call.

Current: self-view is left as is, i.e. if it was on during the call, it remains on after the call; if it was off during the call, it remains off after the call.

On: self-view is switched on when leaving a call.

Video Selfview Default FullscreenMode

Define if the main video source (self-view) shall be shown in full screen or as a small picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting).

Requires user role: ADMIN

Default value: Current

Value space: Off/Current/On

Off: self-view will be shown as a PiP.

Current: The size of the self-view picture will be kept unchanged when leaving a call, i.e. if it was a PiP during the call, it remains a PiP after the call; if it was fullscreen during the call, it remains fullscreen after the call.

On: The self-view picture will be shown in fullscreen.

Video Selfview Default OnMonitorRole

Define which monitor/output to display the main video source (self-view) on after a call. The value reflects the monitor roles set for the different outputs in the Video Output Connector [n] MonitorRole setting.

The setting applies both when self-view is displayed in full screen, and when it is displayed as picture-in-picture (PiP), but only if the Video Monitors setting is set to Dual or Triple.

Requires user role: ADMIN

Default value: Current

Value space: First/Second/Third/Current

First: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to First.

Second: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to Second.

Third: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to Third.

Current: When leaving a call, the self-view picture will be kept on the same output as it was during the call.

Video Selfview Default PIPPosition

Define the position on screen of the small self-view picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting) and fullscreen view is switched off (see the Video Selfview Default FullscreenMode setting).

Requires user role: ADMIN

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the self-view PiP will be kept unchanged when leaving a call.

UpperLeft: The self-view PiP will appear in the upper left corner of the screen.

UpperCenter: The self-view PiP will appear in the upper center position.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear in the center left position.

CentreRight: The self-view PiP will appear in the center right position.

LowerLeft: The self-view PiP will appear in the lower left corner of the screen.

LowerRight: The self-view PiP will appear in the lower right corner of the screen.

Video Selfview OnCall Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video Selfview OnCall Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: self-view is not shown automatically during call setup.

On: self-view is shown automatically during call setup.

Video Selfview OnCall Duration

This setting only has an effect when the Video Selfview OnCall Mode setting is switched On. In this case, the number of seconds set here determines for how long self-view is shown before it is automatically switched off.

Requires user role: ADMIN

Default value: 10

Value space: Integer (1..60)

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

Experimental settings

The Experimental settings are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

Appendices

How to use Touch 10

The Touch 10 user interface and its use are described in full detail in the User guide for the video system.

Indicates whether or not the *Proximity* feature is available.

Tap the upper left corner to access the *System Information* and *Settings*, *Restart* the video system, and activate/deactivate *Standby*, and the *Proximity* and *Do not disturb* modes

Tap ? to contact Help desk, if available.

Tap the *Camera* icon to activate self-view and camera control.

Time of day.

Tap *Dial* to invoke the dial pad.

Tap *Sign In* to log on to a shared video system with your own personal credentials, if available.

Tap *Contacts* to invoke the list of contacts including *Favorites*, *Directory* and *Recents*.

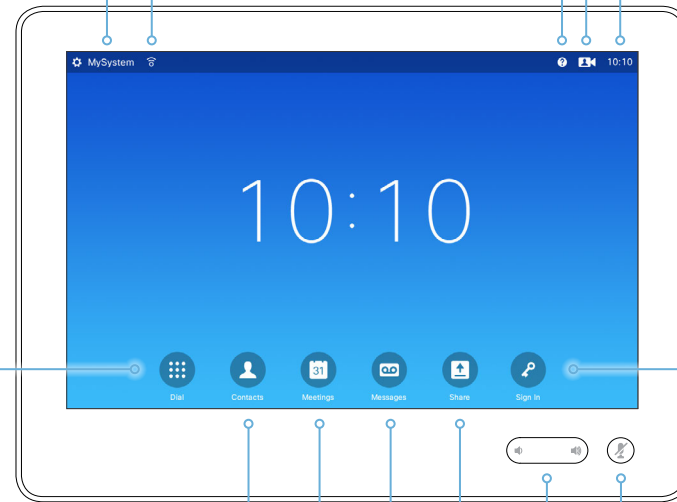
Press the *Microphone* button to mute/unmute microphones.

Tap *Meetings* to invoke a list of upcoming scheduled meetings.

Press and hold the left side of the Volume button to decrease the loudspeaker volume and the right side to increase the volume

Tap *Messages* to invoke the voice mail system, if available.

Tap *Share* to start sharing content and to conduct presentations.



Set up remote monitoring

Requirement:

- *RemoteMonitoring* option

Remote monitoring is useful when you want to control the video system from another location.

Snapshots from input sources appear in the web interface, so you can check the camera view and control the camera without being in the room.



Check whether or not the video system has the *RemoteMonitoring* option

1. Sign in to the web interface.
2. Check the Home page to see if *RemoteMonitoring* is on the list of Installed options.

If not on the list, remote monitoring is not available.

Enable remote monitoring

Install the *RemoteMonitoring* option key. How to install option keys are described in the [Install option keys](#) chapter.

PLEASE BE AWARE THAT IF YOU ENABLE THE REMOTE MONITORING OPTION YOU MUST MAKE SURE THAT YOU COMPLY WITH LOCAL LAWS AND REGULATIONS WITH REGARD TO PRIVACY AND PROVIDE ADEQUATE NOTICE TO USERS OF THE SYSTEM THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS YOUR RESPONSIBILITY TO COMPLY WITH PRIVACY REGULATIONS WHEN USING THE SYSTEM AND CISCO DISCLAIMS ALL LIABILITY FOR ANY UNLAWFUL USE OF THIS FEATURE.

About snapshots

Local input sources

Snapshots of the local input sources of the video system appear on the Call Control page.

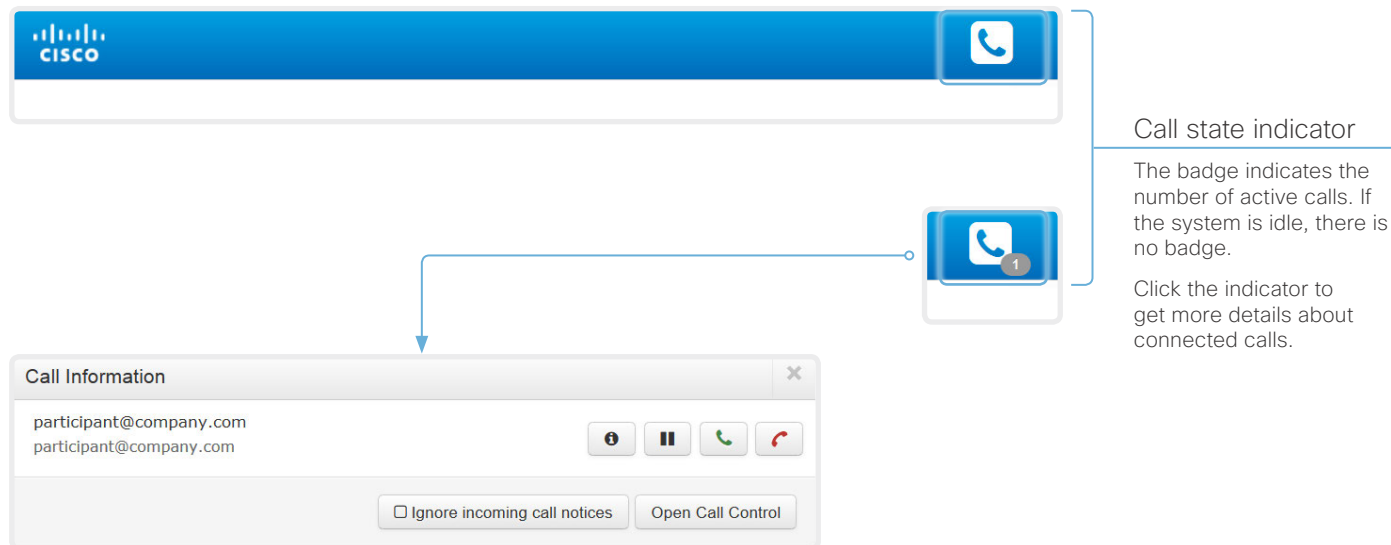
Snapshots appear both when the video system is idle, and when in a call.

Far end snapshots

When in call, you may also see snapshots from the far end camera. It does not matter whether or not the far end video system has the *RemoteMonitoring* option.

Far end snapshots are not displayed if the call is encrypted.

Access call information while using the web interface



Call state indicator

The badge indicates the number of active calls. If the system is idle, there is no badge.

Click the indicator to get more details about connected calls.

About the call state indicator

The call state indicator shows whether the system is in a call or not, and how many calls it is engaged in. You may also be notified about incoming calls.

The call state indicator is available on all pages except the [Call Control](#) page.

Open the Call Information window

Click the *Call state indicator* to open the *Call Information* window manually.

As default, the *Call Information* window pops up automatically when the video system receives a call.

Switch incoming call notifications on or off

Click *Ignore incoming call notices*, to decide whether or not the *Call Information* window should pop up automatically when the video system receives a call.





When the check box is checked, the *Call Information* window will not open automatically.

Open the Call Control page

Click *Open Call Control* to go straight to the *Call Control* page.

Control the call(s)

Relevant control buttons appear in the *Call Information* window. Use the buttons to:

-  Show call details
-  Put the call on hold
-  Answer the call
-  Disconnect the call

Place a call using the web interface (page 1 of 2)

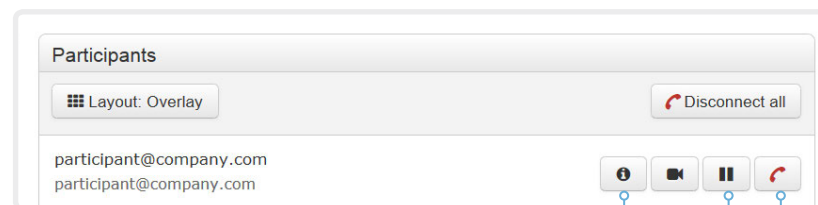
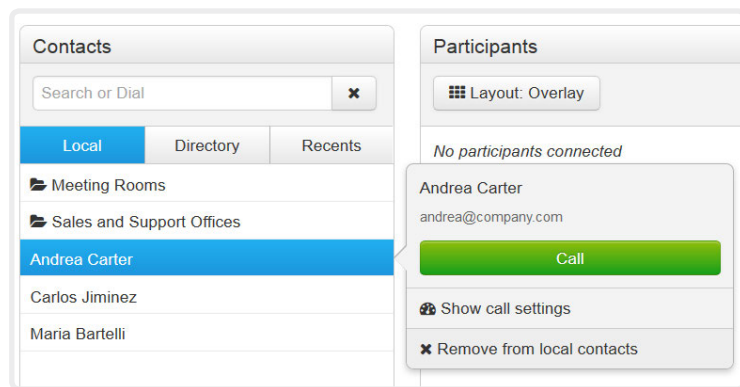
Sign in to the web interface and navigate to [Call Control](#).

Place a call

i Even if the web interface is used to initiate the call, it is the video system (display, microphones and loudspeakers) that is used for the call; it is not the PC running the web interface.

1. Navigate the *Local*, *Directory* or *Recents* lists to find the correct entry; or enter one or more characters in the *Search or Dial* field*. Click the correct contact name.
2. Click [Call](#) in the contact card.

Alternatively, enter the complete URI or number in the *Search and Dial* field. Then click the [Call](#) button that appears next to the URI or number.



Show/hide call details

Click the information button to show details about the call.

Click the button again to hide the information.

Hold and resume a call

Use the **||** button next to a participant's name to put that participant on hold.

To resume the call, use the **▶** button that is present when a participant is on hold.

End a call

If you want to terminate a call or conference, click [Disconnect all](#). Confirm your choice in the dialog that appears.

To disconnect just one participant in a conference, click the button for that participant.

* When searching, matching entries from the *Local*, *Directory* and *Recents* lists will be listed as you type.

Place a call using the web interface (page 2 of 2)

Sign in to the web interface and navigate to [Call Control](#).

Calling more than one

A point-to-point video call (a call involving two parties only) can be expanded to include one more participant on audio-only.

If your system is using the optional built-in MultiSite feature, up to five participants, yourself included, can join the video call (conference). In addition, one more participant can join on audio-only.

Follow the same procedure to call the next conference participant as you did when calling the first participant.

Calling more than one using a conference bridge (CUCM ad hoc conferencing) is not supported from the web interface, even if it is supported by the video system itself.

Adjust the volume

Mute the microphone

Click [Microphone: On](#) to mute the microphone. Then the text changes to [Microphone: Off](#).

Click [Microphone: Off](#) to unmute.



Share content using the web interface

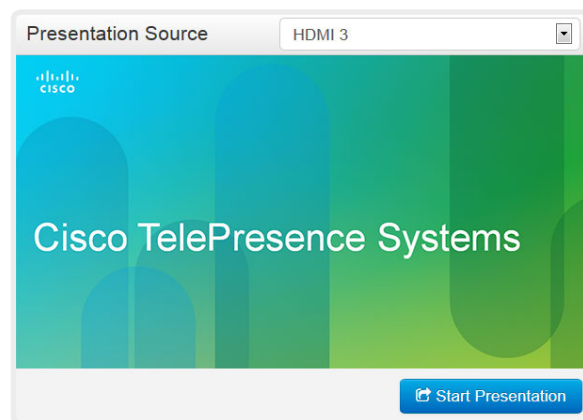
Sign in to the web interface and navigate to [Call Control](#).

Share content

1. Choose which content source to share in the *Presentation Source* drop down list.
2. Click [Start Presentation](#). Then the text changes to [Stop Presentation](#).

Stop content sharing:

Click the [Stop Presentation](#) button that is present while sharing.



Presentation Source drop down list

Choose which input source to share, from the drop down list.

Snapshot area

Shows snapshots of the selected presentation source.

Only available on video systems that have the *Remote Monitoring* option.

About content sharing

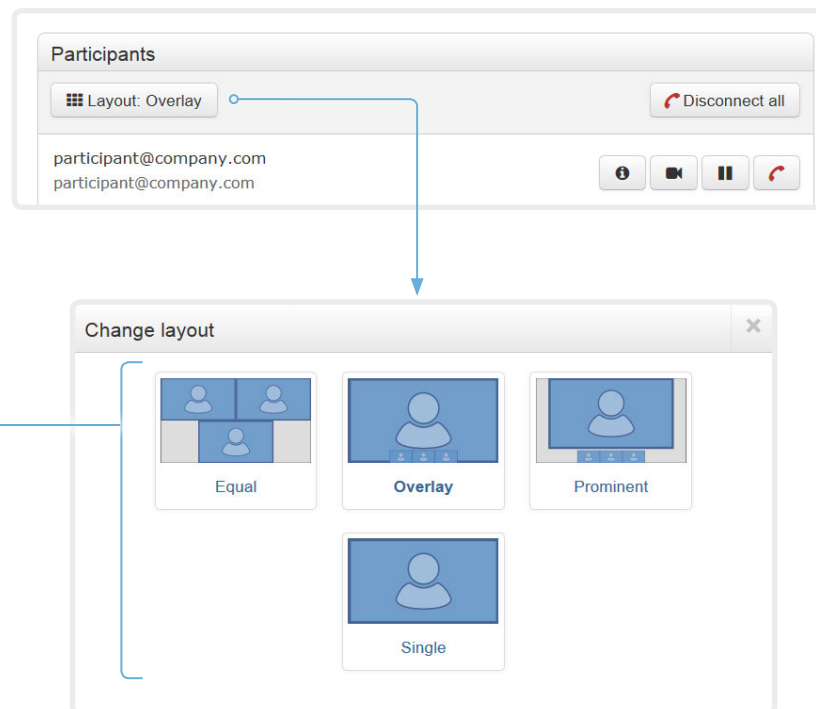
You can connect a presentation source to one of the video inputs of your video system. Most often a PC is used as presentation source, but other options may be available depending on your system setup.

While in a call you can share content with the other participant(s) in the call (far end).

If you are not in a call, the content is shared locally.

Local layout control

Sign in to the web interface and navigate to [Call Control](#).



Change the layout

Click [Change layout](#), and choose your preferred layout in the window that opens.

The set of layouts to choose from depends on the system configurations.

You may change the layout both when idle and in a call.

About layouts

The term layout is used to describe the various ways the videos from the conference participants and a presentation can appear on the screen. Different types of meetings may require different layouts.

Control the local camera(s)

Sign in to the web interface and navigate to [Call Control](#).

Prerequisites

- The [Video > Input > Connector n > CameraControl > Mode](#) setting is switched **On**.
- The camera has pan, tilt or zoom functionality.

Snapshot area

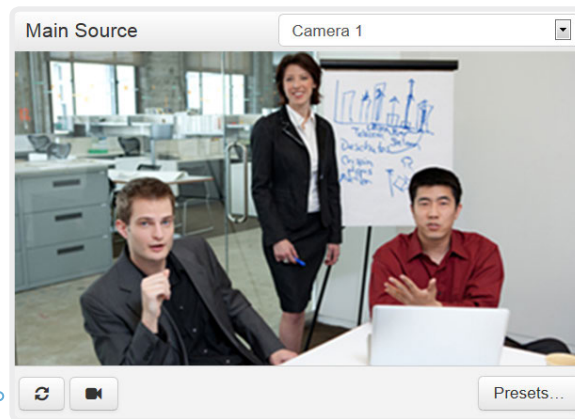
Shows snapshots of the selected main input source.

Only available on video systems that have the *Remote Monitoring* option.

Automatically refresh snapshots

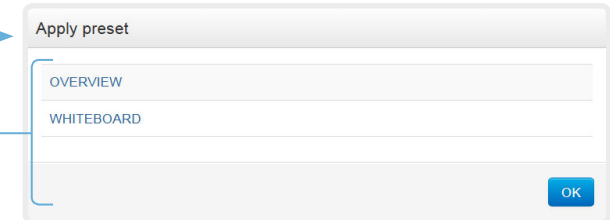
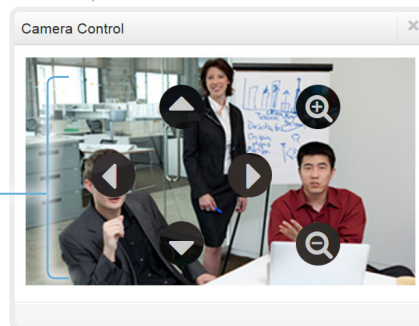
Move the camera using the pan/tilt/zoom controls

1. Choose which camera to control in the *Main Source* drop down list.
2. Click the camera icon to open the camera control window.
Video snapshots from the room are only displayed for video systems that have the *Remote Monitoring* option.
3. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.
Only relevant controls appear in the window.



Main Source drop down list

Choose which camera to control from the drop down list.



Move the camera to a preset position

1. Choose which camera to control in the *Main Source* drop down list.
2. Click [Presets...](#) to open a list of available presets.
If no presets are defined, the button is disabled and named *No presets*.
3. Click a preset's name to move the camera to the preset position.
4. Click **OK** to close the window.

i You cannot use the web interface to define a preset; you should use the Touch controller.

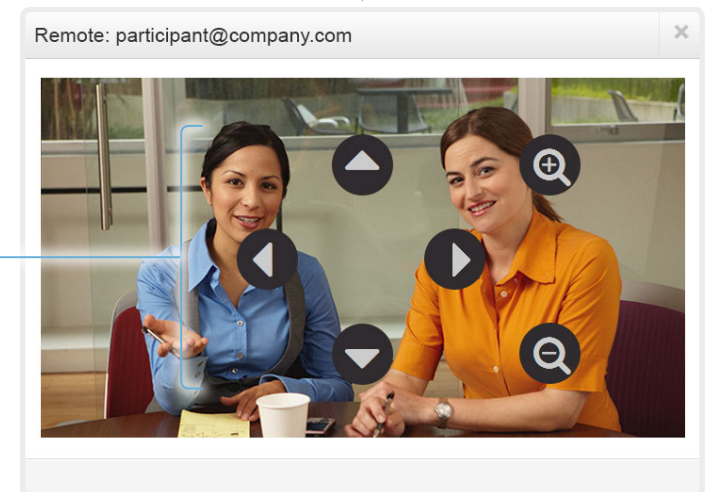
Control the far end camera

Sign in to the web interface and navigate to [Call Control](#).

Prerequisites

While in a call, you can control the remote participant's camera (far end) provided that:

- The [Conference > FarEndControl > Mode](#) setting is switched **On** on the far end video system.
- The far end camera has pan, tilt or zoom functionality. Only the relevant controls will appear.
- The local video system has the *Remote Monitoring* option.



Control the remote participant's camera

1. Click the camera icon to open the remote camera control window.
2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.

If you are not allowed to control the far end camera, the controls will not appear in the image.

Advanced customization of audio and GPIO

The CE Console application (previously TC Console), which is a free software tool that runs on PC/Mac, provides a graphical interface to the advanced customizable features of the codec. CE Console includes the following modules:

GPIO

- Change the behavior of the GPIO, i.e. what the codec should do when pins go high/low

Audio console

- Configure the audio system of the codec.
- Change the default mixing, routing and equalizers
- Set various input and output connector properties

Video composition is not available for any video system in the initial releases of CE Console. Audio console is only available for SX80 in the initial release.

For more details about the functionality, see the user guide included in the CE Console application itself or download the CE Console user guide from <http://www.cisco.com/go/sx-docs>

How to obtain the CE Console application

Download the CE Console application for free from the Cisco DevNet web site. Go to:

► <http://developer.cisco.com/web/telepresence-developer>

Access the video system's XML files

Sign in to the web interface and navigate to [Configuration > API](#).

The XML files are part of the video system's API. They structure information about the system in a hierarchy.

- *Configuration.xml* contains the current system settings (configuration). These settings are controlled from the web interface or from the API (Application Programmer Interface).
- The information in *status.xml* is constantly updated by the video system to reflect system and process changes. The status information is monitored from the web interface or from the API.
- *Command.xml* contains an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- *Valuespace.xml* contains an overview of all the value spaces of system settings, status information, and commands.

Open an XML file

Click the file name to open the XML file.

About the API

The application programming interface (API) is a tool for integration professionals and developers working with the video system. The API is described in detail in the API guide for the video system.

Execute API commands and configurations from the web interface

Sign in to the web interface and navigate to [Configuration > API](#).

Commands (xCommand) and configurations (xConfiguration) can be executed from the web interface. Syntax and semantics are explained in the API guide for the video system.

Execute API commands and configurations

1. Enter a command (xCommand or xConfiguration), or a sequence of commands, in the text area.
2. Click [Execute](#) to issue the command(s).

Execute API commands and configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

Enter commands...

Execute

About the API

The application programming interface (API) is a tool for integration professionals and developers working with the video system. The API is described in detail in the API guide for the video system.

Manage startup scripts

Sign in to the web interface, and navigate to [Configuration > Startup Scripts](#).

List of startup scripts

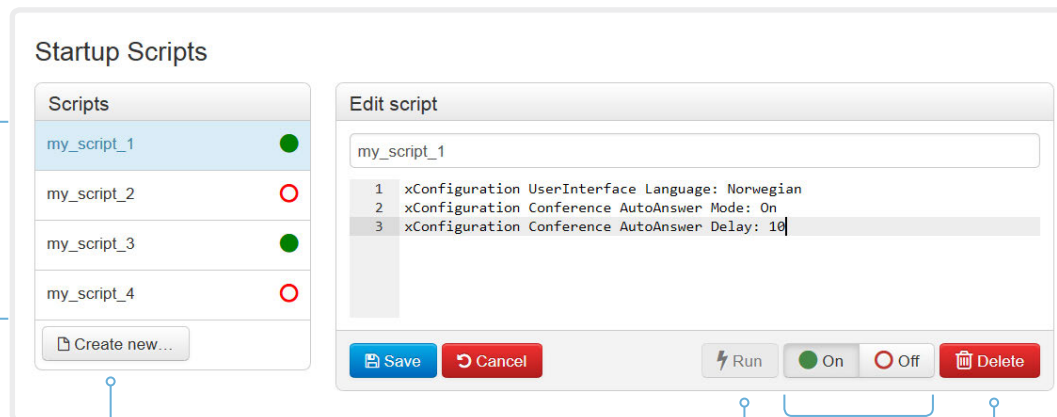
You can create one or more startup scripts*.

A green dot appears next to an active startup script; a red ring appears next to an inactive startup script.

If you have more than one startup script, they will run in the order from top to bottom of the list.

Create a startup script

1. Click [Create new...](#)
2. Enter a name for the startup script in the title input field.
3. Enter the commands (xConfiguration or xCommand) in the command input area. Start each command on a new line.
4. Click [Save](#).
5. Click [On](#) to activate the startup script.



The script names and configurations shown in the illustration serve as examples. You may make your own scripts.

Run a startup script immediately

1. Select the startup script from the list.
2. Click [Run](#).

Both active and inactive startup scripts can be run immediately.

Activate or deactivate a startup script

1. Select the startup script from the list.
2. Click [On](#) to activate, or [Off](#) to deactivate a script.

Active startup scripts will run every time the video system starts up.

Delete a startup script

1. Select the startup script from the list.
2. Click [Delete](#).

About startup scripts

A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure.

A few commands and configurations cannot be placed in a startup script, for example xCommand SystemUnit Boot. It is not possible to save a script that contains illegal commands and configurations.

Syntax and semantics for xCommand and xConfiguration are explained in the API guide for the product.

Serial interface (RS-232)

SX80 has a standard COM-port for serial communication. Connect a standard 9-pin RS-232 serial cable to the COM-port. If the computer does not have a standard serial connector, you need an RS-232 adapter on the computer side.

The serial connection can be used without an IP-address, DNS, or a network.

Parameters:

- Baud rate: Configurable. Default 115200 bps
- Data bits: 8
- Parity: None
- Stop bit: 1

Video system settings

Serial communication is enabled by default. Use the following configuration to change the behavior:

[SerialPort > Mode](#)

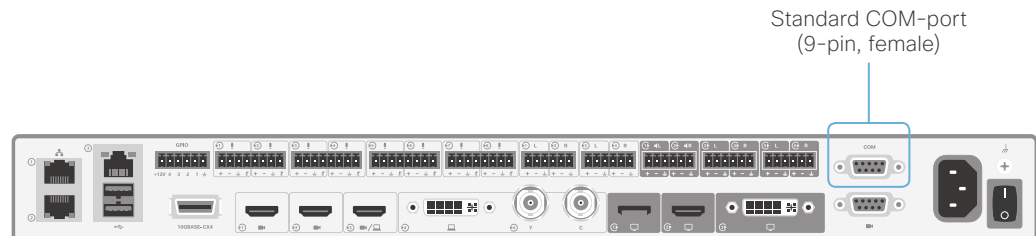
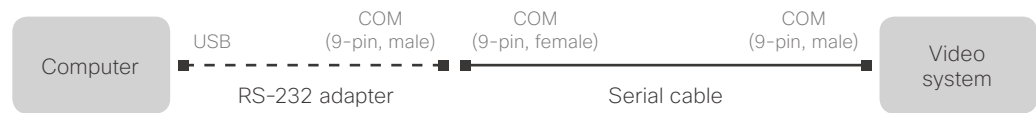
For security reasons, you are asked to sign in before using the serial interface. Use the following setting to change the behavior:

[SerialPort > LoginRequired](#)

We recommend using the default baud rate because the video system may give much feedback. Use the following setting if you want to adjust the baud rate.

[SerialPort > BaudRate](#)

Restart the video system when you have made changes to the serial port settings.



Technical specification (page 1 of 3)

PRODUCT COMPATIBILITY

Fully compatible with standards-compliant telepresence and video systems

SOFTWARE COMPATIBILITY

- Cisco TelePresence Software Version TC7.1 or later
- Collaboration Endpoint Software Version 8.0 or later

BANDWIDTH

H.323 and SIP up to 6 Mbps point-to-point

Up to 6 Mbps total MultiSite bandwidth

MINIMUM BANDWIDTH FOR RESOLUTION / FRAME RATE (H.264)

- 720p30 from 768 kbps
- 720p60 from 1152 kbps
- 1080p30 from 1472 kbps
- 1080p60 from 2560 kbps

FIREWALL TRAVERSAL

- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal
- SIP ICE (Interactive Connectivity Establishment)

VIDEO STANDARDS

- H.261
- H.263
- H.263+
- H.264
- H.265 (SIP)

VIDEO FEATURES

- Advanced screen layouts
- Local auto-layout

VIDEO INPUTS (FIVE INPUTS)

Three HDMI inputs*

Support formats up to maximum 1920 × 1080@60fps, including:

- 1920 × 1080@60 and 59.94 Hz (1080p60)
- 1920 × 1080@50 Hz (1080p50)
- 1920 × 1080@30 and 29.97 Hz (1080p30)
- 1920 × 1080@25 Hz (1080p25)
- 1920 × 1080@24, and 23.97 Hz (1080p24)

- 1280 × 720@60, and 59.94 Hz (720p60)
- 1280 × 720@50 Hz (720p50)
- 720 × 480@60, and 59.94 Hz (480p60)
- 640 × 480@60 Hz (480p60)
- 1280 × 1024@60, and 75 Hz (SXGA)
- 1024 × 768@60, 70, 75, and 85 Hz (XGA)
- 800 × 600@56, 60, 72, 75, and 85 Hz (SVGA)
- 1920 × 1200@50 and 60 Hz (WUXGA)
- 1680 × 1050@60 Hz (WSXGA+)
- 1440 × 900@60 Hz (WXGA+)
- 1280 × 768@60 Hz (WXGA)

One DVI-I input

Analog (VGA or YPbPr); support formats up to maximum 1920 × 1080@60fps (1080p60), including:

- 1920 × 1080@60 Hz (1080p)
- 1280 × 720@60 Hz (720p)
- 1280 × 1024@60 and 75 Hz (SXGA)
- 1280 × 960@60 Hz
- 1024 × 768@60, 70, 75, and 85 Hz (XGA)
- 1680 × 1050@60 Hz (WSXGA+)
- 1440 × 900@60 Hz (WXGA+)
- 1280 × 800@60 Hz (WXGA)
- 1280 × 768@60 Hz (WXGA)

Digital (DVI-D); support formats up to maximum 1920 × 1080@60fps, including:

- 1920 × 1080@60, 59.94 Hz (1080p60)
- 1920 × 1080@50 Hz (1080p50)
- 1920 × 1080@30, 29.97 Hz (1080p30)
- 1920 × 1080@25 Hz (1080p25)
- 1920 × 1080@24, 23.97 Hz (1080p24)
- 1280 × 720@60, 59.94 Hz (720p60)
- 1280 × 720@50 Hz (720p50)
- 720 × 480@60, 59.94 Hz (480p60)
- 640 × 480@60 Hz (480p60)
- 1280 × 1024@60, 75 Hz (SXGA)
- 1024 × 768@60, 70, 75, 85 Hz (XGA)
- 800 × 600@56, 60, 72, 75, 85 Hz (SVGA)
- 1680 × 1050@60 Hz (WSXGA+)
- 1440 × 900@60 Hz (WXGA+)
- 1280 × 768@60 Hz (WXGA)

One Composite/S-Video Input (BNC Connectors)

- PAL/NTSC

Extended Display Identification Data (EDID)

VIDEO OUTPUTS (THREE OUTPUTS)

Two HDMI outputs* and one DVI-I output

Supports formats up to maximum 1920 × 1080@60fps (1080p60), including:

- 1920 × 1080@60 Hz (1080p60)
- 1920 × 1080@50 Hz (1080p50)
- 1280 × 720@60 Hz (720p60)
- 1280 × 720@50 Hz (720p50)

VESA Monitor Power Management

Extended Display Identification Data (EDID)

Supports encode/decode video formats up to maximum 1920 × 1080@60fps (HD1080p60), including:

- 176 × 144@30 frames per second (fps) (QCIF)
- 352 × 288@30 fps (CIF)
- 512 × 288@30 fps (w288p)
- 576 × 448@30 fps (448p)
- 768 × 448@30 fps (w448p)
- 704 × 576@30 fps (4CIF)
- 1024 × 576@30 fps (w576p)
- 1280 × 720@30 fps (720p30)
- 1920 × 1080@30 fps (1080p30)
- 640 × 480@30 fps (VGA)
- 800 × 600@30 fps (SVGA)
- 1024 × 768@30 fps (XGA)
- 1280 × 1024@30 fps (SXGA)
- 1280 × 768@30 fps (WXGA)
- 1440 × 900@30 fps (WXGA+)
- 1680 × 1050@30 fps (WSXGA+)
- 512 × 288@60 fps (w288p60)
- 768 × 448@60 fps (w448p60)
- 1024 × 576@60 fps (w576p60)
- 1280 × 720@60 fps (720p60)
- 1920 × 1080@60 fps (1080p60)

AUDIO STANDARDS

- 64 kbps and 128 kbps AAC-LD
- G.722
- G.722.1
- G.711
- G.729AB

AUDIO FEATURES

- High quality 20 kHz audio
- Eight separate acoustic echo cancellers
- Eight-port audio mixer
- Eight assignable equalizers
- Automatic gain control (AGC)
- Automatic noise reduction
- Active lip synchronization

AUDIO INPUTS (15 INPUTS)

- Eight microphones, 48V phantom powered, Euroblock connector, each with separate echo cancellers and noise reduction; all microphones can be set for balanced line level
- Four balanced line level inputs, Euroblock connector
- Three HDMI inputs, digital, stereo (from PC/DVD)*

AUDIO OUTPUTS (EIGHT OUTPUTS)

- Six balanced line level outputs, Euroblock connector
- Two HDMI outputs*

DUAL STREAM

- H.239 (H.323) dual stream
- BFCP (SIP) dual stream
- Support for resolutions up to 1080p30, independent of main stream resolution

MULTIPOINT SUPPORT

- Five-way embedded SIP/H.323 MultiPoint, ref. MultiSite
- Cisco Ad-Hoc Conferencing (requires Cisco Unified Communications Manager (CUCM), Cisco TelePresence Server and Conductor)
- Cisco Conferencing Active Control

* HDMI version 1.4

Technical specification (page 2 of 3)

MULTISITE FEATURES (EMBEDDED MULTIPOINT)

- Five-way 720p30, three-way and four-way 1080p30 MultiSite
- Full individual audio and video transcoding
- Individual layouts in MultiSite continuous presence
- H.323/SIP/VoIP in the same conference
- Support for Presentation (H.239/BFCP) from any participant at resolutions up to 1080p15
- Best Impression (automatic continuous presence layouts)
- H.264, encryption and dual stream from any site
- IP downspeeding
- Dial in and dial out
- Conference rates up to 6 Mbps

PROTOCOLS

- H.323 and SIP (dual call stack support)
- ISDN (requires Cisco TelePresence ISDN Link)

EMBEDDED ENCRYPTION

- H.323 and SIP point-to-point
- Standards-based: H.235 v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Supported in dual stream

IP NETWORK FEATURES

- DNS lookup for service configuration
- Differentiated services (QoS)
- IP adaptive bandwidth management (including flow control)
- Auto gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 DTMF tones in H.323

- RFC 4733 DTMF tones in SIP
- Date and time support via NTP
- Packet loss based downspeeding
- URI dialing
- TCP/IP
- DHCP (Dynamic Host Configuration Protocol)
- IEEE 802.1x network authentication
- IEEE 802.1q VLAN
- IEEE 802.1p QoS and class of service
- ClearPath

IPv6 NETWORK SUPPORT

- Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS and DiffServ
- Support for static IP address assignment, stateless autoconfiguration and DHCPv6

CISCO UNIFIED COMMUNICATIONS MANAGER

(requires Cisco UCM version 8.6 or later)

- Native registration with Cisco Unified Communications Manager (CUCM)
- Basic CUCM provisioning
- Firmware upgrade from CUCM
- Cisco Discovery Protocol and DHCP option 150 support
- Basic telephony features such as hold, resume, transfer, and corporate directory lookup

SECURITY FEATURES

- Management using HTTPS and SSH
- IP administration password
- Administration menu password
- Disable IP services
- Network settings protection

NETWORK INTERFACES

- One LAN/Ethernet (RJ-45) 10/100/1000 Mbps
- Two LAN/Ethernet (RJ-45) interfaces to be used for Cisco TelePresence peripherals

OTHER INTERFACES

- Two USB host for future use
- GPIO

SYSTEM MANAGEMENT

- Support for the Cisco TelePresence Management Suite (TMS)
- Management via embedded Telnet, SSH, XML, and SOAP
- Full application programming interface (APIs)
- Remote software upload via web server, SCP, HTTP, and HTTPS
- One RS-232 for local control and diagnostics
- Support for Cisco TelePresence Touch 10

DIRECTORY SERVICES

- Support for local directories (Favorites)
- Corporate directory (through CUCM and Cisco TMS)
- Server directory supporting LDAP and H.350 (requires Cisco TMS)
- Call history with received, placed and missed calls with date and time

POWER

- Autosensing power supply
- 100-240 VAC, 50/60 Hz
- Power consumption under normal operating conditions as defined in IEC 60950-1: 99 W

OPERATING TEMPERATURE AND HUMIDITY:

- Ambient temperature: 32°F to 104°F (0°C to 40°C)
- Relative humidity (RH): 10% to 90%

STORAGE AND TRANSPORT TEMPERATURE:

- -4°F to 140°F (-20°C to 60°C) at RH 10% to 90% (non-condensing)

DIMENSIONS

- Width: 442 mm / 17.4 in.
- Height: 44 mm / 1.7 in.
- Depth: 310 mm / 12.2 in.
- Weight: 3.65 kg / 8.05 lbs

Technical specification (page 3 of 3)

APPROVALS AND COMPLIANCE

EU/EEC

Directive 2006/95/EC (Low Voltage Directive)

- Standard IEC/EN 60950-1

Directive 2004/108/EC (EMC Directive)

- Standard EN 55022, Class A
- Standard EN 55024
- Standard EN 61000-3-2/-3-3

Directive 2011/65/EU (RoHS)

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

USA

Approved according to UL 60950-1

Complies with FCC CFR 47 15B, Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

Approved according to CAN/CSA C22.2 No. 60950-1

This Class A digital apparatus complies with Canadian ICES-003

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

All specifications are subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

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

November 2015

Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2460 Internet protocol, version 6 (IPv6) specification
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3388 Grouping of Media Lines in the Session Description Protocol (SDP)
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3891 The SIP "Replaces" Header
- RFC 3892 Referred-By Mechanism
- RFC 3960 Early Media
- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
- RFC 4028 Session Timers in SIP
- RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
- RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4235 An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4583 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams draft-ietf-bfcpbis-rfc4583bis-00 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4587 RTP Payload Format for H.261 Video Streams
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5104 Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)
- RFC 5168 XML Schema for Media Control
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5389 Session Traversal Utilities for NAT (STUN)
- RFC 5577 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 5589: SIP Call Control Transfer
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5768 Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6156 Traversal Using Relays around NAT (TURN) Extension for IPv6
- RFC 6184 RTP Payload Format for H.264 Video
- draft-ietf-payload-rtp-h265-02 RTP Payload Format for High Efficiency Video Coding

User documentation on the Cisco web site

User documentation for the Cisco TelePresence products is available at ► <http://www.cisco.com/go/telepresence/docs>

Choose a product category in the right pane until you find the correct product. This is the path you have to follow:

*TelePresence Integration Solutions >
Cisco TelePresence SX Series*

Alternatively, use the following short-link to find the documentation: ► <http://www.cisco.com/go/sx-docs>

The documents are organized in the following categories:

Install and Upgrade > Install and Upgrade Guides

- *Installation guides*: How to install the product
- *Getting started guide*: Initial configurations required to get the system up and running
- *RCSI guide*: Regulatory compliance and safety information

Maintain and Operate > Maintain and Operate Guides

- *Getting started guide*: Initial configurations required to get the system up and running
- *Administrator guide*: Information required to administer your product
- *Deployment guide for TelePresence endpoints on CUCM*: Tasks to perform to start using the video system with the Cisco Unified Communications Manager (CUCM)

Maintain and Operate > End-User Guides

- *User guides*: How to use the product
- *Quick reference guides*: How to use the product
- *Physical interface guide*: Details about the codec's physical interface, including the connector panel and LEDs.

Reference Guides | Command references

- *API reference guides*: Reference guide for the Application Programmer Interface (API)

Reference Guides > Technical References

- *CAD drawings*: 2D CAD drawings with measurements

Configure > Configuration Guides

- *CE Console user guide*: How to use the CE Console application, which provides a graphical interface to advanced customizable features of the codec.

Design > Design Guides

- *Video conferencing room guidelines*: General guidelines for room design and best practice
- *Video conferencing room guidelines*: Things to do to improve the perceived audio quality

Software Downloads, Release and General Information > Licensing Information

- *Open source documentation*: Licenses and notices for open source software used in this product

Software Downloads, Release and General Information > Release Notes

- *Software release notes*

Intellectual property rights

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco product security overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at <http://www.bis.doc.gov/policiesandregulations/ear/index.htm>.

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ► <http://www.cisco.com/go/offices>

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA