

Collaboration Endpoint software version 8.3  
JANUARY 2017



# Administrator guide

for Cisco TelePresence SX10 Quick Set

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

<b>Introduction.....</b>	<b>4</b>
User documentation and software .....	5
What's new in CE8.....	6
SX10 Quick Set at a glance.....	20
Power On and Off .....	21
LED indicators .....	22
How to administer the video system.....	23
<b>Configuration .....</b>	<b>28</b>
User administration .....	29
Change the system passphrase .....	30
Set a PIN code for the on-screen Settings menu .....	31
System configuration .....	32
Add a sign in banner .....	33
Manage the service certificates of the video system.....	34
Manage the list of trusted certificate authorities (CAs) .....	35
Set up secure audit logging .....	36
Manage pre-installed certificates for CUCM via Expressway provisioning.....	37
Delete CUCM trust lists.....	38
Change the persistency mode.....	39
Set strong security mode .....	40
Set up Intelligent Proximity for content sharing .....	41
Adjust the video quality to call rate ratio.....	46
Packet loss resilience - ClearPath.....	47
Choose wallpaper .....	48
Choose a ringtone and set the ringtone volume .....	49
Manage local contacts.....	50
<b>Peripherals.....</b>	<b>51</b>
Real-time communication requirements for displays .....	52
Connect the Touch 10 controller .....	53
Extend the number of input sources.....	55
<b>Maintenance .....</b>	<b>56</b>
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
<b>System settings .....</b>	<b>70</b>
Overview of the system settings .....	71
Audio settings .....	75
CallHistory settings .....	77
Cameras settings.....	78
Conference settings .....	80
FacilityService settings.....	84
H323 settings.....	85
Logging settings .....	88
Network settings.....	89
NetworkServices settings.....	96
Peripherals settings .....	101
Phonebook settings .....	103
Provisioning settings.....	104
Proximity settings.....	107
RoomReset settings.....	108
RTP settings.....	109
Security settings .....	110
SerialPort settings.....	112
SIP settings .....	113
Standby settings .....	117
SystemUnit settings.....	119
Time settings .....	120
UserInterface settings.....	123
UserManagement settings.....	125
Video settings .....	127
Experimental settings .....	134

<b>Appendices.....</b>	<b>135</b>
How to use the remote control and the on-screen user interface .....	136
How to use Touch 10 .....	137
Set up remote monitoring .....	138
Access call information while using the web interface.....	139
Place a call using the web interface .....	140
Share content using the web interface.....	142
Local layout control.....	143
Control a local camera.....	144
Control a far end camera.....	145
Add in-room controls to Touch 10 .....	146
Manage startup scripts .....	147
Access the video system's XML files .....	148
Execute API commands and configurations from the web interface .....	149
Serial interface.....	150
Technical specification.....	151
Supported RFCs .....	153
User documentation on the Cisco web site.....	154
Cisco contacts .....	155



## Chapter 1

# Introduction

## User documentation and software

### Products covered in this guide

- Cisco TelePresence SX10 Quick Set

This guide does not cover information on Cisco Spark registered systems. For more information on Cisco Spark room systems, visit:

► <https://help.webex.com/community/cisco-cloud-collab-mgmt>

### 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*.

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

### Downloading the user documentation

Visit the Cisco web site regularly for updated versions of the guides:

► <http://www.cisco.com/go/sx-docs>

### Cisco Project Workplace

Explore the Cisco Project Workplace to find inspiration and guidelines when preparing an office or meeting room for video conferencing:

► <http://www.cisco.com/go/projectworkplace>

### 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

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 (CE8) 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 upgrade path



**Before upgrading, it is important to consider the upgrade requirements of CE8;** otherwise upgrading to CE8.0 or later can leave you with a non-functional deployment that requires you to downgrade.

Refer to the software release notes, and the

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

## New features and improvements in CE8.3

### Control of an external video switch with additional input sources

You can customize our touch user interfaces to include input sources that are connected to third-party external video switches. These *external* input sources will appear and behave just as a video source that is connected directly to the video system. You don't have to swap cables or change the physical input source manually.

The number of external input sources you can create depends on how many inputs the video switches allow. Cisco recommends maximum 50 sources.

The video switch must be supported by a third-party control system, for example from Crestron or AMX, which can interact with the video system's xAPI. It is the control system, not the video system, that controls the video switch.

For more information about how to customize the user interface, and how to use the xAPI to set up this feature, refer to the user guide: ► <http://www.cisco.com/go/in-room-control-docs>

### ActiveControl in CMS 2.1 hosted conferences

ActiveControl is a SIP-only feature that has been supported for a while for video systems in Cisco TelePresence Server hosted conferences.

From CE8.3 ActiveControl is also supported in CMS 2.1 hosted conferences. It is enabled by default on the video system, and can be used as long as it is supported by the infrastructure as well (auto-negotiation).

New ActiveControl functionality:

- When the video system is muted from the server side, the mute indicator is shown on screen and the microphone's mute LED is lit.
- Best effort encryption is used by default.
- An *automatic* layout is introduced as default. Who is shown in the *automatic* layout is based on recent active speakers.
- Recording status indicator shown on screen.
- ActiveControl functionality available from the Call Control page on the web interface, for example participant list, participant mute indicator, and drop participant button.

### Media channel details available in the xAPI

Media channels contains information about audio, video and data for ongoing calls. You can monitor the channel rate, packet loss, jitter, video frame rate, and more from the xAPI.

Sign in to the xAPI as an admin user and run `xStatusMediaChannels` to see the media channel details. You can also check the media channel status on the Status page in the web interface.

### HTTP feedback in JSON format

HTTP feedback can be sent in JSON (JavaScript Object Notation) format for third-party feedback interpreters, as an alternative to XML (eXtensible Markup Language) .

TMS uses XML by default, and does not support JSON formatted feedback.

### Configurable network speed

You can configure the Ethernet link speed from the web interface or the xAPI. This is in alignment with other video systems running CE software.

You can choose to autonegotiate the link speed (default), or force it to:

- 10 Mbps half-duplex
- 10 Mbps full-duplex
- 100 Mbps half-duplex
- 100 Mbps full-duplex

In general, we recommend not to change from the default value, where the video system negotiates with the network to set the speed automatically.

### Keypad for DTMF tones available on the web interface

We have added a keypad to the Call Control page of the web interface. The keypad is available when in call, and can be used to send DTMF tones to the far end when required.

### Wireless sharing from laptop enabled by default when using Cisco Proximity

The *Content sharing from clients* service, which allows a laptop to share content to a video system via Proximity, is now enabled by default. The other services (*Content sharing to clients* and *Basic call control*) must be explicitly enabled by the administrator.

As before, Proximity mode must be on in order to pair a laptop to a video system through the Cisco Proximity desktop client. Pairing is required before you can use any of the wireless sharing services.

### New languages

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

## New features and improvements in CE8.2

### LDAP user management

You can register users with ADMIN role from an external LDAP service to grant them access to the video system's web interface and API. This allows for centralized management of ADMIN users. The LDAP server can be configured from the web interface. Authenticating users with the USER role using LDAP is not supported.

LDAP configuration can be set from CUCM. If the video system requires a certificate for login from LDAP, it must be uploaded to the video system manually as CUCM is unable to provision certificates.

### Administrator credentials not needed for remote pairing to a Touch 10

You no longer need to enter administrator credentials when you remote pair a Touch 10 controller to a video system. All user credentials can be used for this purpose. The administrator doesn't have to visit the site or provide administrator credentials in order to pair or re-pair a touch controller to a video system.

Un-pairing the Touch 10 controller and changing the administrator settings still require ADMIN credentials.

### Additional entry points for in-room controls

In-room controls are extended to allow multiple panels, which are available depending on the context. These are the possible entry points: *Global* (introduced in CE8.1), *Homescreen* and *In-Call*. The *Homescreen* entry point is in the home screen icon tray, next to the Dial, Contacts, and Share buttons. The *In-Call* entry point is in the icon tray that is accessible when the video system is in a call. The *Global* entry point is in the status bar (as in CE8.1).

New panel icons have also been added.

### Cisco Spark support

CE8.2 introduces support for Cisco Spark activation for SX10 (CTS-SX10-K9), SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, MX800 Dual, DX70 and DX80. A video system registered to the Cisco Spark service can be used together with Cisco Spark mobile and desktop applications.

To register to Cisco Spark:

- Touch 10 must be directly paired (Touch 10 is not supported for Spark registered SX10N, SX10, SX20, DX70 and DX80)
- Encryption Option key must be installed (Does not apply to DX70 and DX80)

When the video system is activated on Cisco Spark, it downloads the newest version of Cisco Spark Room OS.

Cisco Spark Room OS does not have the same management capabilities as Collaboration Endpoint Software as its web and command line interfaces are locked. The Room System is managed by Cisco and if there are any issues, contact Cisco Technical Assistance center through the Cisco Spark mobile application or from the management portal.

For more information on the Cisco Spark Room OS and its features see: ► <https://help.webex.com>

### H.323 support

SX10 can now register to an H.323 Gatekeepers and make calls using the H.323 protocol.

### Cisco Proximity updates

The application name has changed from Proximity to Cisco Proximity.

The latest release includes the following improvements:

- First time use tutorial for desktop application
- Updated look for the user interface
- Improved pairing experience
- Increased visibility on the user's desktop
- Better information and handling of failure scenarios
- Link to support forums on the client

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).

### Touch 10 user interface changes

A visual update has been applied to the Setup and Pairing Wizard on the Touch 10. The Touch 10 has a new GUI when registered to Cisco Spark, which is similar to the Cisco TelePresence SX10 on-screen user interface. If the endpoint is registered to on-premise infrastructure, the Touch 10 controller has the same user interface as CE8.1.



## Default option keys removed

Option keys for features that have become default on all Cisco TelePresence video systems are removed. The functionalities provided by these options are still present, but the keys are no longer needed.

Removed option keys:

- PremiumResolution
- NaturalPresenter
- DualDisplay
- HighDefinition

Option keys that are still available:

- Encryption
- MultiSite
- RemoteMonitoring

## New user role: *RoomControl*

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

## Added language support

We have added support for Canadian French (Français – Canada) to the on-screen display and Touch controller menus.

## New features and improvements in CE8.1

### In-room control

With the In-Room Control feature you can customize the Touch 10 user interface to allow control of peripherals in your meeting room, for example lights and blinds. You get a consistent user experience when the video system and other peripherals in the room are controlled from the same device.

You can create the user interface extensions for Touch 10 with the In-Room Control Editor. This is an easy to use drag-and-drop editor that you launch from the video system's web interface. You can also work offline with a stand-alone version of the editor. The editor is available free of charge; no option key is required.

A third-party control system with hardware drivers for the peripherals, for example Crestron, AMX, Apple HomeKit, or Android is required to control the peripherals. The control system connects to the video system's API, listens for events and executes the programmed actions.

For more information about setting up the In-Room Control feature, refer to the user guide: ► <http://www.cisco.com/go/in-room-control-docs>

### User interface update

A new visual design for the Touch 10 and on-screen display user interfaces is introduced.

### Overscan adjustment from the on-screen display

If you operate the video system with a TRC6 remote control, you can now adjust the overscan settings also from the on-screen display. Previously you had to use the web interface or API.

You can adjust the overscan settings both in the setup wizard and by selecting *Screen Adjustment* in the settings menu. This way you can adjust the image to fit the screen in scenarios where parts of the image are not visible.

Most screens have built-in settings to adjust the image, and these settings should be attempted first.

### Cisco Spark support

Collaboration Endpoint Software 8.1 introduces support for Cisco Spark activation for SX10 (CTS-SX10N-K9). An SX10 registered to the Cisco Spark service can be used together with Cisco Spark mobile and desktop applications.

When the SX10 is activated on Cisco Spark, it downloads the newest version of Cisco Spark Room OS.

Cisco Spark Room OS does not have the same management capabilities as Collaboration Endpoint Software as its web and command line interfaces are locked. The Room System is managed by Cisco and if there are any issues, contact Cisco Technical Assistance center through the Cisco Spark mobile application or from the management portal.

For more information on the Cisco Spark Room OS and its features see: ► <https://help.webex.com>

### Change in audio only avatar behavior

Full screen avatar for audio only participants has been removed. The audio only participants continue to be visible in the filmstrip during a call.

### Intelligent Proximity updates

Sharing a presentation with the Cisco Intelligent Proximity desktop application renders the laptop's mouse pointer on screen. This feature requires the latest version of Cisco Proximity for Desktop together with CE8.1.

When using a video system with the TRC6 remote control, users can temporarily enable and disable the Intelligent Proximity services. This was previously only available on the Touch 10.

### Direct content sharing

You can configure the video system to automatically share a presentation with the far-end participants when connecting a presentation source during a call. In previous software versions, sharing a presentation with the far-end always required you to manually select *Share* with the remote control or Touch controller.

If a presentation source is already connected when the call starts, you must manually select *Share* to share the presentation with the far-end.

For further details, refer to the *Video Input Connector [n] PresentationSelection* setting.

## New features and improvements in CE8.0

### 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).

### 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.

### PIN code protection

The on-screen Advanced Settings menu can be PIN code protected to prevent unauthorized users from changing the configuration of the video system.

### Resolution changes

Collaboration Endpoint Software only supports displays that support 16:9 resolution.

Supports 1080p presentation sharing both locally and in a call, at 5 frames per second.

### 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

- 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.
- MediaNet is no longer supported.

## System configuration changes in CE8.3

### New configurations

Network [1] Speed

Peripherals Profile ControlSystems

Standby AudioMotionDetection

### Configurations that are removed

SIP Ice OfferTcpCandidates

Moved to Experimental

### Configurations that are modified

H323 Encryption KeySize

**OLD:** Default value: Max1024bit

**NEW:** Default value: Min1024bit

Logging External Server Port

**OLD:** Default value: 0

**NEW:** Default value: 514

Network [1] \*

**OLD:** User role: Admin

**NEW:** User role: Admin, User

Proximity Services ContentShare FromClients

**OLD:** Default value: Disabled

**NEW:** Default value: Enabled

Standby BootAction

**OLD:** User role: Admin

**NEW:** User role: Admin, User

Standby WakeupAction

**OLD:** User role: Admin

**NEW:** User role: Admin, User

UserInterface/Language

**Change:** EnglishUK and SpanishLatin added to value space

## System configuration changes in CE8.2

### New configurations

Conference DefaultCall Protocol  
H323 Authentication LoginName  
H323 Authentication Mode  
H323 Authentication Password  
H323 CallSetup Mode  
H323 Encryption KeySize  
H323 Gatekeeper Address  
H323 H323Alias E164  
H323 H323Alias ID  
H323 NAT Address  
H323 NAT Mode  
H323 PortAllocation  
NetworkServices H323 Mode  
Peripherals Profile Cameras  
UserManagement LDAP Mode  
UserManagement LDAP Server Address  
UserManagement LDAP Server Port  
UserManagement LDAP Encryption  
UserManagement LDAP MinimumTLSVersion  
UserManagement LDAP VerifyServerCertificate  
UserManagement LDAP Admin Filter  
UserManagement LDAP Admin Group  
UserManagement LDAP Attribute  
UserManagement LDAP BaseDN

### Configurations that are removed

None

### Configurations that are modified

Logging External Server Address  
**OLD:** String (0, 64)  
**NEW:** String (0, 255)  
NetworkServices NTP Server [1..3] Address  
**OLD:** String (0, 64)  
**NEW:** String (0, 255)  
NetworkServices SNMP Host [1..3] Address  
**OLD:** String (0, 64)  
**NEW:** String (0, 255)  
Provisioning Connectivity  
**OLD:** User Role: ADMIN  
**NEW:** User Role: ADMIN, USER  
Provisioning ExternalManager Address  
**OLD:** User Role: ADMIN  
**NEW:** User Role: ADMIN, USER  
Provisioning ExternalManager AlternateAddress  
**OLD:** User Role: ADMIN  
**NEW:** User Role: ADMIN, USER  
Provisioning ExternalManager Domain  
**OLD:** User Role: ADMIN  
**NEW:** User Role: ADMIN, USER  
Provisioning ExternalManager Path  
**OLD:** User Role: ADMIN  
**NEW:** User Role: ADMIN, USER

#### Provisioning ExternalManager Protocol

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Provisioning HttpMethod

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Provisioning LoginName

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Provisioning Mode

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Proximity Mode

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Proximity Services CallControl

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Proximity Services ContentShare FromClients

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Proximity Services ContentShare ToClients

**OLD:** User Role: ADMIN

**NEW:** User Role: ADMIN, USER

#### Security Audit Server Address

**OLD:** String (0, 64)

**NEW:** String (0, 255)

#### 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.

#### UserInterface Language

**OLD:** Arabic / Catalan / ChineseSimplified / ChineseTraditional / Czech / Danish / Dutch / English / Finnish / French / German / Hebrew / Hungarian / Italian / Japanese / Korean / Norwegian / Polish / PortugueseBrazilian / Russian / Spanish / Swedish / Turkish

**NEW:** Arabic / Catalan / ChineseSimplified / ChineseTraditional / Czech / Danish / Dutch / English / Finnish / French / FrenchCanadian / German / Hebrew / Hungarian / Italian / Japanese / Korean / Norwegian / Polish / PortugueseBrazilian / Russian / Spanish / Swedish / Turkish

#### Video Input Connector [n] InputSourceType

**OLD:** PC / camera / document\_camera / mediaplayer / other / whiteboard

**NEW:** PC / camera / desktop / document\_camera / mediaplayer / other / whiteboard

#### Video Input Connector [n] PresentationSelection

**OLD:** AutoShare / Manual / OnConnect

**NEW:** AutoShare / Desktop / Manual / OnConnect

## System configuration changes in CE8.1

### New configurations

Audio Input Microphone [2] EchoControl Dereverberation  
 Audio Input Microphone [2] EchoControl Mode  
 Audio Input Microphone [2] EchoControl NoiseReduction  
 Audio Input Microphone [2] Mode  
 Audio Output Line [n] Delay DelayMs  
 Audio Output Line [n] Delay Mode  
 Logging External Mode  
 Logging External Protocol  
 Logging External Server Address  
 Logging External Server Port  
 Security Session MaxSessionsPerUser  
 Security Session MaxTotalSessions  
 SIP Ice OfferTcpCandidates

### Configurations that are removed

Conference Presentation RelayQuality  
 Conference VideoBandwidth MainChannel Weight  
 SIP Turn BandwidthProbe

### Configurations that are modified

Cameras Camera [n] Flip  
**OLD:** <Auto / Off / On>  
**NEW:** <Auto>  
 Conference DefaultCall Rate  
**OLD:** Default value: 1920  
**NEW:** Default value: 3072

Conference DoNotDisturb DefaultTimeout

**OLD:** Integer (0..1440)

**NEW:** Integer (1..1440)

Conference VideoBandwidth PresentationChannel Weight

**OLD:** Integer (1..10)

Default value: 2

**NEW:** Integer (1..9)

Default value: 5

FacilityService Service [1] Name

**OLD:** Default value: ""

**NEW:** Default value: "Live Support"

Phonebook Server [1] Type

**OLD:** <CUCM / Off / TMS / VCS>

**NEW:** <CUCM / Off / Spark / TMS / VCS>

Provisioning Mode

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

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

SIP DisplayName

**OLD:** String (0, 255)

**NEW:** String (0, 550)

Standby BootAction

**OLD:** Default value: DefaultCameraPosition

**NEW:** Default value: RestoreCameraPosition

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.

UserInterface Wallpaper

**OLD:** <Custom / None>

Default value: None

**NEW:** <Auto / Custom / None>

Default value: Auto

Video Input Connector [n] PresentationSelection

**OLD:** <Manual / OnConnect>

**NEW:** <AutoShare / Manual / OnConnect>

All configurations that were associated with the *USER* user role in CE8.0, are now associated with both the *USER* and *ADMIN* user roles. So all configurations that were designated for the *USER* user role, are now included with the *ADMIN* role too.



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

### New configurations

Audio Input Microphone [2] Level  
CallHistory 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.*

Conference [1] Multipoint Mode  
Network [1] DHCP RequestTFTPServerAddress  
NetworkServices CTMS Encryption  
NetworkServices CTMS Mode  
NetworkServices HTTPS Mode  
NetworkServices Medianet Metadata  
SIP AuthenticateTransferror  
SIP OCSP \*  
SIP Profile [1] Outbound  
SIP Profile [1] Proxy [n] Discovery  
SystemUnit CallLogging Mode  
SystemUnit MenuLanguage

Time OlsonZone  
UserInterface OSD LanguageSelection  
UserInterface TouchPanel DefaultPanel  
Video AllowWebSnapshots  
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 SelfviewPosition  
Video Wallpaper

### Configurations that are modified

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 / CUCM>  
Default value: TMS  
**NEW:** <Off / VCS / TMS / CUCM>  
Default value: Off

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>

### 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] CallProtocolIPStack

**Renamed to:** Conference CallProtocolIPStack

#### 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] 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] 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

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 PIPPosition

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

## SX10 Quick Set at a glance

The Cisco TelePresence SX10 Quick Set is an all-in-one unit designed to video-enable small collaboration spaces.

It is a high quality unit that combines camera and codec into a compact device that is mounted over a standard flat-panel display. It can be connected to power and LAN through a single cable for both power and Ethernet (PoE).

The camera has a wide-angle field of view, and provides good overview even in small spaces. High-definition video is enabled with 1080p30 resolution.

### Features and benefits

- Optimal definition up to 1080p30 with content sharing at WXGAp5.
- Wide angle 83° horizontal field of view with 5x zoom (optical and digital).
- Ready-to-use unit with Power over Ethernet (PoE).
- Integrated microphone, and optional external Cisco TelePresence Table Microphone 20.
- Operation using TRC6 remote control (default), or 10 inch Touch controller (optional).
- Energy efficient with low power consumption (EU Class B).
- Registers with Cisco Unified Communications Manager (UCM), Cisco TelePresence Video Communication Server (VCS), and Cisco Spark.



SX10 Quick Set is delivered with a TRC6 remote control. You may order the Cisco TelePresence Touch 10 controller as an option



SX10 Quick Set mounted on top of a standard flat-panel display

## Power On and Off

### Power On/Off with the Power button

The power button, with LED indicator, is placed on the front as shown in the illustration.



#### Switch on

If the video system does not start automatically, press the power button gently, and hold for a few seconds.

The LED is lit while the video system starts up.

#### Switch off

Press the power button gently and hold until the light goes out.

#### Enter/exit standby mode

Press the power button briefly. It takes a few seconds before the unit enters standby.

### Power Off or restart the system remotely

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


#### Restart the system

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

It takes a few minutes before the system is ready for use.

#### Power Off the system

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

 You cannot power the system on again remotely.

### Restart and standby using the remote control or Touch controller

#### Restart the system

1. Select the settings icon (cogwheel) on the home screen, or in the status bar of the Touch controller.
2. Select [System Information > Restart](#) with the remote control, or [Settings > Restart](#) on the Touch controller.
3. Select [Restart](#) again to confirm your choice.

#### Enter/exit standby mode

1. Select the settings icon (cogwheel) on the home screen, or in the status bar of the Touch controller.
2. Select [Standby](#).

## LED indicators



### Status LED

The status LED is a circle around the power button. The normal LED color is white. A red light indicates hardware failure.

*Normal operation (not standby):*

Steady light.

*In standby mode:*

The LED pulsates slowly.

*No network connection:*

The LED repeatedly flashes twice.

*During startup (boot):*

The LED flashes.

### Camera LED

The camera LED is just above the camera lens.

*Incoming call:*

The LED flashes.

*In call:*

Steady light.

## How to administer the video system (page 1 of 5)

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"> <li>• Used by the web interface of the video system</li> <li>• Non-secure (HTTP) or secure (HTTPS) communication</li> <li>• HTTP: <i>Enabled</i> by default</li> <li>• HTTPS: <i>Enabled</i> by default</li> </ul>	<a href="#">NetworkServices &gt; HTTP &gt; Mode</a>  Restart the video system for changes to take effect
Telnet	<ul style="list-style-type: none"> <li>• Non-secure TCP/IP connection</li> <li>• <i>Disabled</i> by default</li> </ul>	<a href="#">NetworkServices &gt; Telnet &gt; Mode</a>  You do not need to restart the video system. It may take some time for changes to take effect
SSH	<ul style="list-style-type: none"> <li>• Secure TCP/IP connection</li> <li>• <i>Enabled</i> by default</li> </ul>	<a href="#">NetworkServices &gt; SSH &gt; Mode</a>  You do not need to restart the video system. It may take some time for changes to take effect
Serial interface (RS-232)	<ul style="list-style-type: none"> <li>• Connect to the video system with a cable. IP-address, DNS, or a network is not required</li> <li>• <i>Enabled</i> by default</li> <li>• For security reasons, you are asked to sign in by default (<a href="#">SerialPort &gt; LoginRequired</a>)</li> </ul>	<a href="#">SerialPort &gt; Mode</a>  Restart the video system for changes to take effect



If all access methods are disabled (set to **Off**), you can no longer configure the video system. You are not able to re-enable (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 5)

## 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.

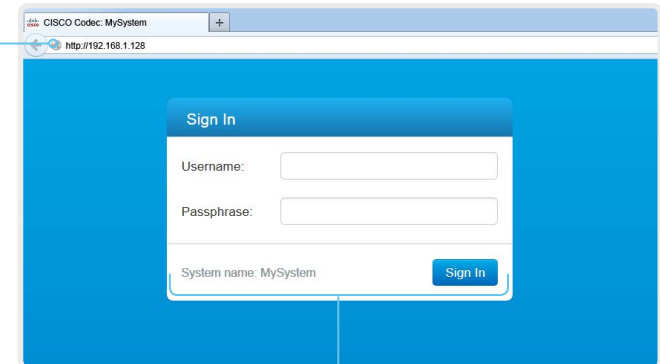
### Connect to the video system

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



#### How to find the IP address

1. Select the settings icon (cogwheel) on the home screen, or in the status bar of the Touch controller.
2. Select [System Information](#) with the remote control, or [Settings > System Information](#) on the Touch controller.



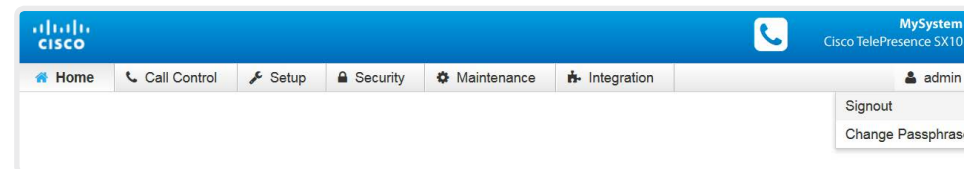
### Sign in

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.

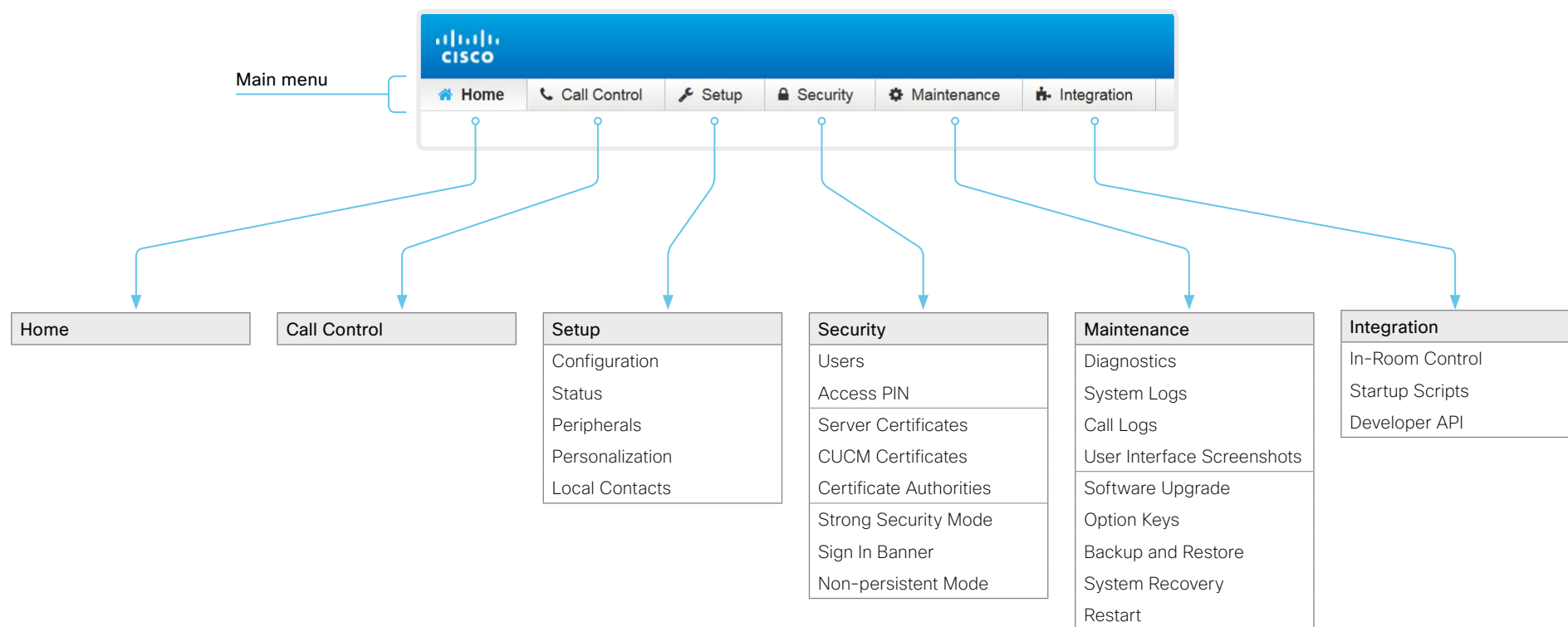


How to administer the video system (page 3 of 5)

## 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 5)

## Settings available on the Touch controller

You have access to 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 settings icon (cogwheel) in the status bar 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.

Settings
Ringtone & Sound
Camera Control
Main Source Selection
Display
Language
System Information
Call Status
Diagnostics
Restart
Administrator >

**Available to all users**

Sign in to the video system's web interface, and navigate to [Setup > Configuration](#).

Use the [UserInterface > UserPreferences](#) setting to decide whether to keep these settings available for all users, or to move them to the passphrase protected area.

Settings
System Information
Call Status
Diagnostics
Restart
Administrator >

**Available to all users**

Administrator Settings
Date, Time & Location
Call Details
Provisioning
Pairing
IP & VLAN - Codec
Network Status - Codec
IP & VLAN - Touch
Network Status - Touch
SIP
H323
Security
EMC Resilience
Reset

**Protected by passphrase**

Administrator Settings
Ringtone & Sound
Camera Control
Main Source Selection
Display
Language
Date, Time & Location
Call Details
Provisioning
Pairing
IP & VLAN - Codec
Network Status - Codec
IP & VLAN - Touch
Network Status - Touch
SIP
H323
Security
EMC Resilience
Reset

**Protected by passphrase**

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

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

[UserInterface > UserPreferences](#): Off

How to administer the video system (page 5 of 5)

## Settings available when using the remote control

You have access to the following information and settings on-screen when you use the TRC6 remote control:

- System information
- Warnings and error messages
- Restart of the video system
- Loudspeakers and microphones check, default camera preset and screen adjustment, presentation sharing test
- Basic settings for language, time zone, network and provisioning (service activation)
- Extended logging
- Factory reset

### Access system information and settings

1. Select the settings icon (cogwheel) on the home screen.
2. Select [System Information](#) to find system information, potential issues, and a *Restart* button.
3. Then, select [Settings](#) for system adjustments and basic configurations.

You may be prompted for a PIN code to open this menu. Consult the ► [Set a PIN code for the on-screen Settings menu](#) section for more details.

Consult the Getting Started Guide for your video system for more details.



## Chapter 2

# Configuration

## User administration

You have to sign in to get access to the web and command line interfaces, and the Administrator settings on the Touch controller. You can assign different roles to users, to determine what they should have access to.

### The default user account

The video system 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 [Security > Users](#).
2. Click [Add new user...](#)
3. Fill in the *Username*, *Passphrase* and *Repeat passphrase* input fields.  
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 client certificates for authentication.
4. Check the appropriate *Roles* check boxes.  
If you assign the ADMIN role to a user, enter your own passphrase in the *Your passphrase* input field for verification.
5. Set the *Status* to **Active** to activate the user.
6. Click [Create User](#).  
Use the [Back](#) button to leave without making any changes.

### Edit an existing user account

If you make changes to a user that holds the Admin role, you must always enter your own passphrase in the *Your passphrase* input field for verification.

#### Change the user privileges

1. Sign in to the web interface, and navigate to [Security > Users](#).
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 [Security > Users](#).
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 [Security > Users](#).
2. Click the appropriate user in the list.
3. Click [Delete user...](#) and confirm when prompted.

### About user roles

A user account may hold one or a combination of *user roles*. A user account with full access rights, like the default *admin* user, should possess the ADMIN, USER and AUDIT roles.

These are the *user roles*:

**ADMIN:** A user with this role can create new users, change most settings, make calls, and search the contact lists. 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.

**ROOMCONTROL:** A user with this role can create in-room controls. The user has access to the In-room control editor and corresponding development tools.

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

## 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.

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

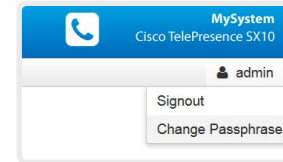
You can create many user accounts for the video system.

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 [Security > Users](#).
2. Click the appropriate user in the list.
3. Enter the new passphrase in the *Passphrase* and *Repeat passphrase* input fields.  
If the user holds the Admin role, you must enter your own passphrase in the *Your passphrase* input field for verification.
4. Click [Change Passphrase](#) to save the change.  
Use the [Back](#) button to leave without making any changes.

## Set a PIN code for the on-screen Settings menu

When you use the TRC6 remote control, you have access to an on-screen *Settings* menu.

We recommend that you set a PIN code for the on-screen *Settings* menu, to prevent unauthorized users from changing the configuration of the video system.

### Set a PIN code

1. Sign in to the web interface, and navigate to [Security > Access PIN](#).
2. Enter a PIN code in the input field, and click [Set PIN](#).  
The PIN can only contain numbers.

### Clear the PIN code

1. Sign in to the web interface, and navigate to [Security > Access PIN](#).
2. Click [Clear PIN](#).

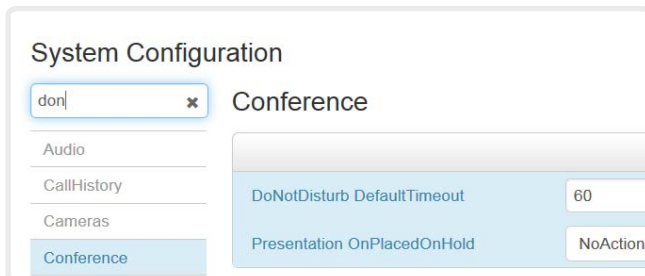
## System configuration

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

### Find a system setting

#### Search for settings

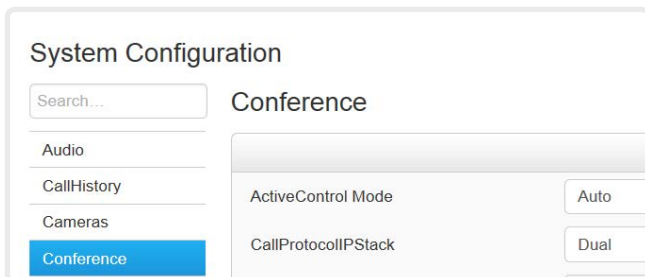
Enter as many letters as needed in the search field. All settings that contain these letters are shown in the right pane. Settings that have these letters in their value space are also shown.



The screenshot shows the 'System Configuration' page. On the left, there is a search bar with 'don' entered and a category list with 'Conference' selected. The right pane shows a list of settings under the 'Conference' category: 'DoNotDisturb DefaultTimeout' with a value of '60' and 'Presentation OnPlacedOnHold' with a value of 'NoAction'.

#### 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.

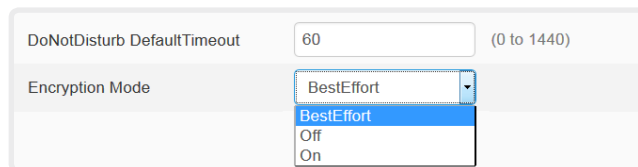


The screenshot shows the 'System Configuration' page. On the left, the 'Conference' category is selected in the category list. The right pane shows settings for the 'Conference' category: 'ActiveControl Mode' with a value of 'Auto' and 'CallProtocolIPStack' with a value of 'Dual'.

### 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.

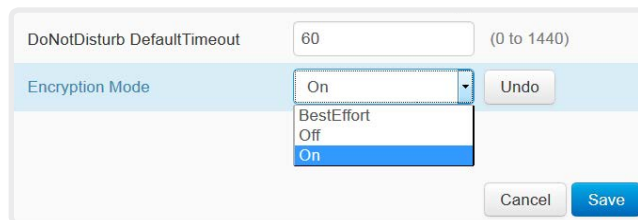


The screenshot shows a close-up of the 'Encryption Mode' setting. The input field displays 'BestEffort' and a drop-down arrow is visible. The drop-down menu is open, showing the following options: 'BestEffort', 'Off', and 'On'.


#### 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.



The screenshot shows a close-up of the 'Encryption Mode' setting. The input field now displays 'On'. The drop-down menu is still open, showing 'BestEffort', 'Off', and 'On'. The 'Save' button is visible at the bottom right of the setting card.

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.

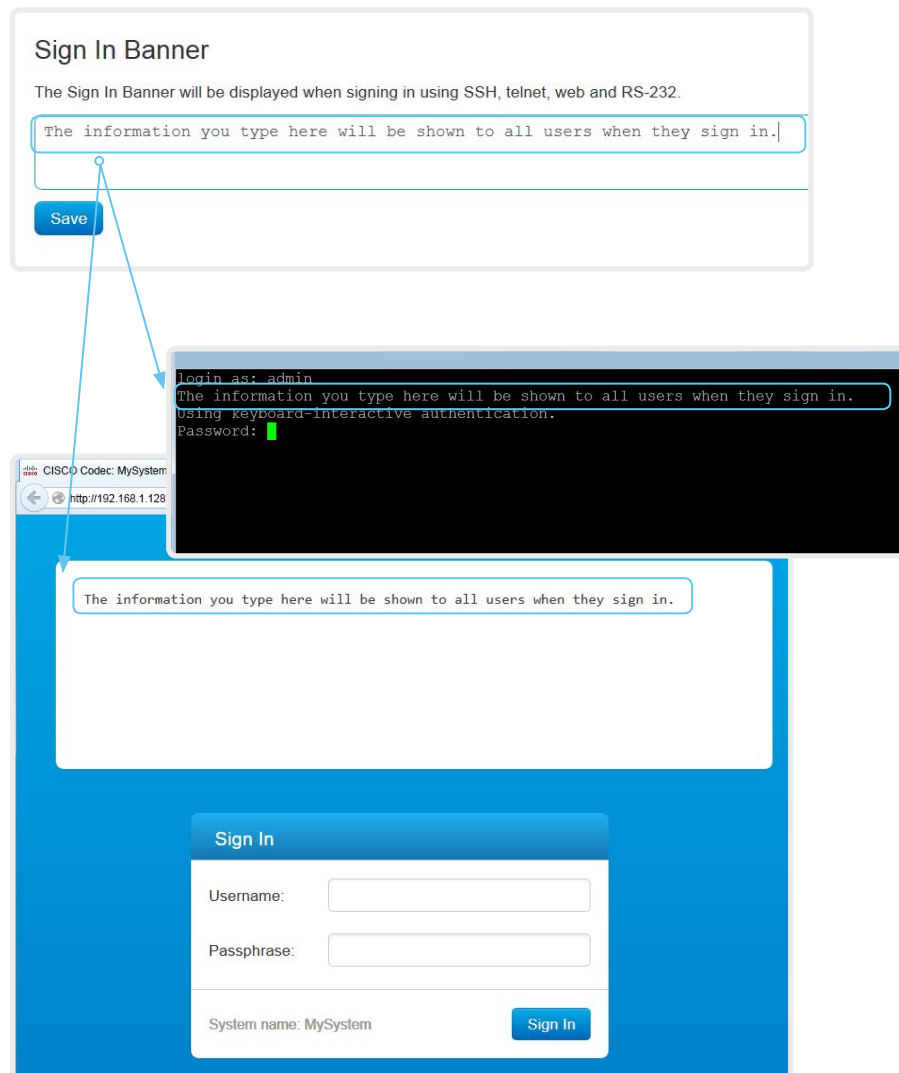
You can read more about user administration and user roles in the [User administration](#) chapter.



## Add a sign in banner

Sign in to the web interface, and navigate to [Security > 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 is shown when the user signs in to the web interface or the command line interface.

## Manage the service certificates of the video system

Sign in to the web interface and navigate to [Security > Service Certificates](#).

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 service 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 and Off buttons to enable or disable a certificate for the different services.

Use the corresponding button to view or delete a certificate.

### 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.

### Service Certificates

Certificate	Issuer	HTTPS server	SIP	802.1X	Audit log		
Certificate_A	CertificateAuthority_A	<input checked="" type="button" value="On"/>	<input type="button" value="Off"/>	<input type="button" value="Off"/>	<input type="button" value="Off"/>	<input type="button" value="Delete..."/>	<input type="button" value="View Certificate"/>
Certificate_B	CertificateAuthority_B	<input type="button" value="Off"/>	<input type="button" value="Off"/>	<input type="button" value="Off"/>	<input type="button" value="Off"/>	<input type="button" value="Delete..."/>	<input type="button" value="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.

## Manage the list of trusted certificate authorities (CAs)

Sign in to the web interface, navigate to [Security > Certificate Authorities](#), and open the [Custom 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 [Add certificate authority...](#) to store the new CA certificates on the video system.

### Certificate Authorities

Custom CAs
Preinstalled CAs

Certificate	Issuer	
CA_Certificate_1	Issuer_1	Delete... View Certificate

#### Add Certificate Authority

CA file
Browse...
No file selected.

This system supports PEM formatted files (.pem) with one or more CA certificates within the file.

Add certificate authority...

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 [Setup > 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.

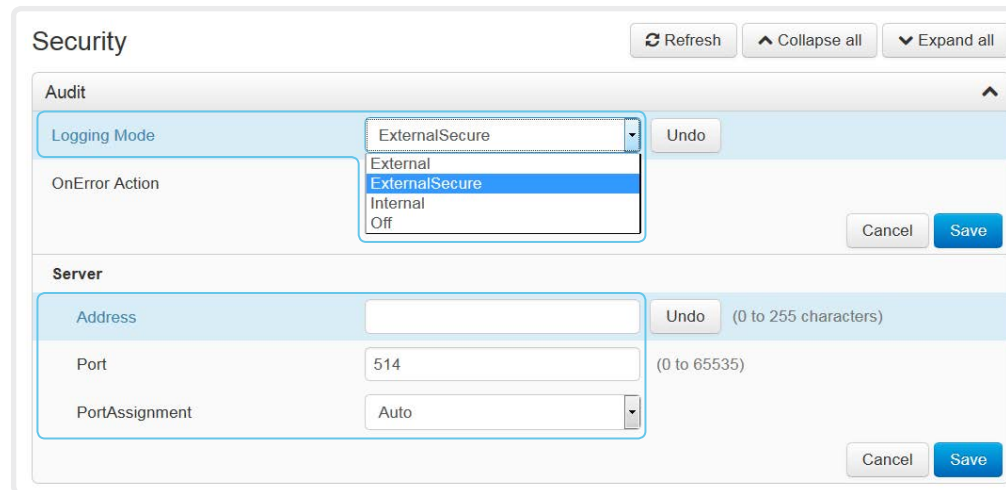
2. Find the [Audit > Server](#) settings, and enter the [Address](#) of the audit server.

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. At the top, there are buttons for 'Refresh', 'Collapse all', and 'Expand all'. Below this is the 'Audit' section, which includes a 'Logging Mode' dropdown menu currently set to 'ExternalSecure'. Other options in the dropdown are 'External', 'ExternalSecure' (highlighted), 'Internal', and 'Off'. There is an 'OnError Action' field and an 'Undo' button. Below the 'Audit' section is the 'Server' section, which includes an 'Address' text field with an 'Undo' button and a character count '(0 to 255 characters)'. It also has a 'Port' text field with the value '514' and a character count '(0 to 65535)', and a 'PortAssignment' dropdown menu set to 'Auto'. At the bottom right of the 'Server' section are 'Cancel' and 'Save' buttons.

### 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 [Security > Certificate Authorities](#), and open the [Preinstalled CAs](#) tab.

### View or disable certificates

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

Certificate Authorities

Custom CAs

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	<a href="#">Details...</a>	✓	<a href="#">Disable</a>
Certificate_02	Issuer_2	<a href="#">Details...</a>	✓	<a href="#">Disable</a>
Certificate_03	Issuer_3	<a href="#">Details...</a>	✓	<a href="#">Disable</a>

[Disable All](#)

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



As an alternative to using the pre-installed certificates, you can append the certificates 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.

## 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 [Security > CUCM Certificates](#).

### 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.

## Change the persistency mode

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

### Check the persistency status

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

Alternatively, you can navigate to [Setup > Status > Security > Persistency](#) to see the status.

### Change the persistency settings

All persistency settings are set to **Persistent** by default. You only have to change the settings to make them **Non-persistent**.

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 you switched to Non-persistent mode, are NOT cleared or deleted.

### Persistency mode

Configurations, call history, internal logs, local phonebook (local directory and favorites list), and IP connectivity information are stored by default. Because all persistency settings are set to **Persistent**, a system restart does not delete this information.

Generally, we recommend you NOT to change the persistency settings. Only change to **Non-persistent** mode if you have to prevent users from being able to see or traceback to any 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 placed and received calls (call history)
- Internal log files
- Changes to the local contacts or favorites list
- All IP related information (DHCP) from the last session



Information that was stored before changing to Non-persistent mode is not automatically cleared or deleted. You must factory reset the video system to delete such information.

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

## Set strong security mode

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

### 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.

#### 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...](#)

#### 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.

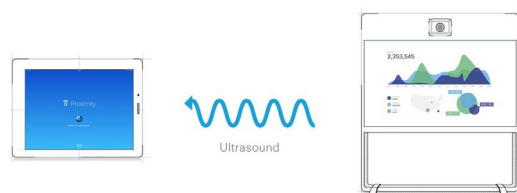
Strong security mode sets very strict passphrase requirements, and requires all users to change their passphrase on the next sign in.



## Set up Intelligent Proximity for content sharing (page 1 of 5)

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
DX70, DX80	3

### Proximity services

*Place calls and control the video system:*

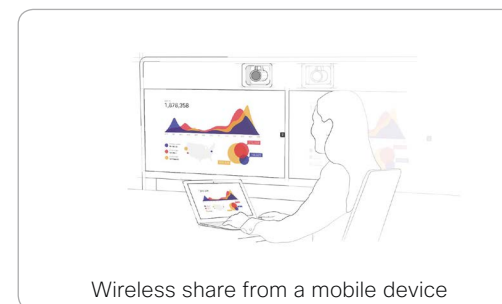
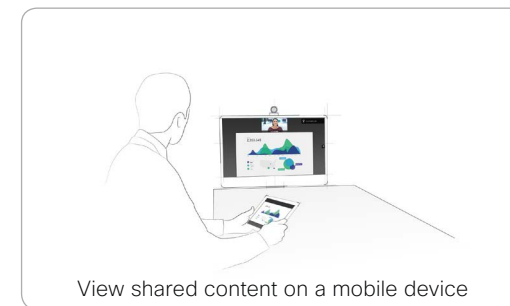
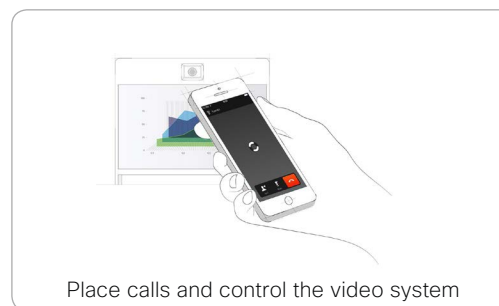
- Dial, mute, adjust volume, hang up
- Available on smartphones and tablets (iOS and Android)

*View shared content on a mobile device:*

- View shared content, review previous slides, save selected slides
- Available on smartphones and tablets (iOS and Android)
- For DX70 and DX80, this service is available only when in a call

*Wireless share from a desktop client:*

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



## Set up Intelligent Proximity for content sharing (page 2 of 5)

### 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](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.

## Set up Intelligent Proximity for content sharing (page 3 of 5)

### Ultrasound emission

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

Use the [Proximity > Mode](#) setting to switch the Proximity feature – and thereby also ultrasound emission – **On** and **Off**.

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

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.

*SX10N and MX Series:*

- The ultrasound sound pressure level is below 75 dB at a distance of 50 cm or more from the loudspeaker.

*DX70 and DX80:*

- The ultrasound sound pressure level is below 75 dB at a distance of 20 cm or more from the loudspeaker.

*SX10, SX20, and SX80:*

- We are not able to control the ultrasound sound pressure level because these systems emit ultrasound on third-party loudspeakers.

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

### Headsets

*DX70, DX80, and SX10N:*

You can always use a headset with these systems because:

- DX70 and DX80 have dedicated headset outputs, on which we never emit ultrasound.
- SX10N has a built-in loudspeaker for ultrasound, so ultrasound is never emitted on the HDMI and loudspeaker outputs.

*SX10, SX20, SX80, or an MX Series:*

- We strongly recommend you to switch off ultrasound emission if you use a headset with these video systems (set [Proximity > Mode](#) to **Off**). Then you *cannot* use the Proximity feature.

Since these systems don't have dedicated headset outputs, we are not able to control the sound pressure level from the connected headsets.

### SX10 versus SX10N

Cisco TelePresence SX10 Quick Set comes in two versions: SX10 and SX10N.

SX10N has a built-in loudspeaker for ultrasound, while SX10 use the same speakers (3<sup>rd</sup> party) for ultrasound as for other audio signals.

### Find which version you have

*SX10* or *SX10N* is part of the following strings:

- Check the PID field on the rating label at the rear of the video system
- Navigate to [Setup > Status](#) in the web interface and check the [SystemUnit > Hardware > UDI](#) status.

## Set up Intelligent Proximity for content sharing (page 4 of 5)

### Enable Proximity services

1. Sign in to the web interface, and navigate to [Setup > 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. Only *Wireless share from a mobile device* is enabled by default.

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 desktop client:*

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

### Temporarily disable the Proximity services

In sessions or meetings where you want to prevent devices in the room from receiving content, you can use the video system's user interface to temporarily disable the Proximity services.



The video system will continue to transmit ultrasound pairing messages during such sessions. This ensures that clients will know about a nearby video system, and can give the user an explanation why he cannot connect.

1. Select the settings icon (cogwheel) on the home screen, or in the status bar of the Touch controller to open the dropdown panel.
2. Switch Proximity on or off with the toggle button.

### The Proximity indicator

You will see a Proximity indicator on both the main display and the Touch controller when Proximity is switched **On**, and at least one Proximity service is enabled.

The Proximity indicator has two states:



Proximity services are available for use.



Proximity services are temporarily disabled. Use the toggle button in the settings dropdown panel to make them available again.

### About Proximity

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.

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

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

Provided that you have verified that Proximity is suitable in your setup, Cisco recommends – for the best user experience – that Proximity always is switched **On**\*

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

\* SX10: We recommend *not* to use a headset, if you have switched **on** Proximity (ultrasound).  
SX10N: You can always use a headset.

## Set up Intelligent Proximity for content sharing (page 5 of 5)

### 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.

### 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 organization. Refer to:

► <http://www.cisco.com/web/siteassets/legal/privacy.html>

You can use the Touch controller to temporarily disable the Proximity services. This is useful in sessions or meetings where you want to prevent mobile devices in the room from receiving content.

You cannot temporarily disable Proximity if you use the TRC6 remote control.

### 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. Applies only to SX10, not to SX10N.
- Check the speaker volume. The volume control on a speaker itself (not the volume controlled with 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. Applies only to SX10, not to SX10N.
- Some Windows laptops are not able to record sound in the ultrasound frequency range (20kHz-22kHz). This can be due to frequency limitations with the sound card, 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*).

#### Cannot share content from a laptop

- For content sharing to work, the video system and the laptop must be on the same network. For this reason Proximity sharing might fail if your video system is connected to your company network via Expressway, and your laptop is connected via VPN (VPN client dependent).

### 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.

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

1. Go to [Video > Input > Connector n > Quality](#) and set the video quality parameter to **Motion** (skip this step for Connector 1 (internal camera)).
2. Go to [Video > Input > Connector n > OptimalDefinition > Profile](#) and choose the preferred optimal definition profile.

### 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.

## 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).

## Choose wallpaper

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

### Choose wallpaper

Choose a wallpaper from the list.  
The active wallpaper is highlighted.

### Upload a custom wallpaper

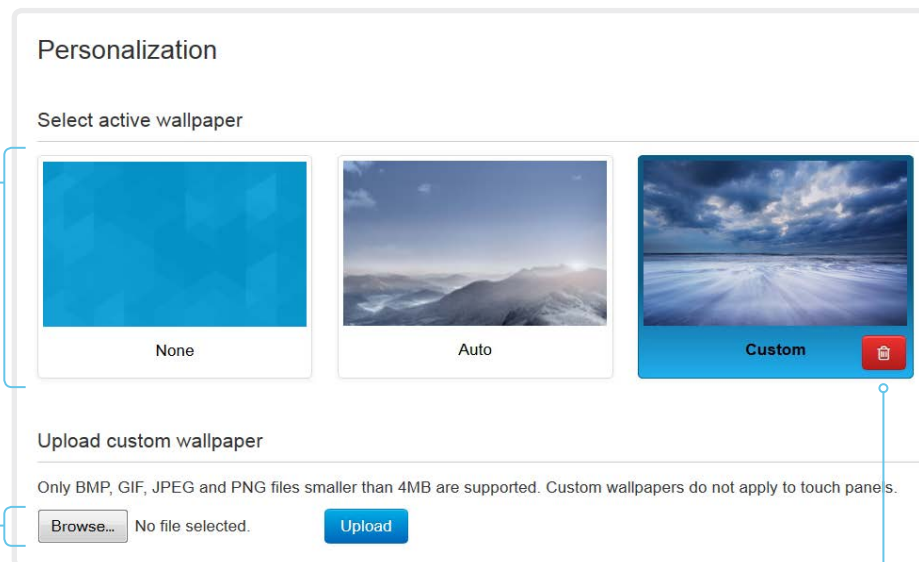
Overwrites any old custom wallpaper.

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.



The screenshot shows the 'Personalization' section of a web interface. Under 'Select active wallpaper', there are three options: 'None' (blue square), 'Auto' (landscape image), and 'Custom' (landscape image with a red delete icon). The 'Custom' option is highlighted with a blue border. Below this, the 'Upload custom wallpaper' section contains a message: 'Only BMP, GIF, JPEG and PNG files smaller than 4MB are supported. Custom wallpapers do not apply to touch panels.' It also features a 'Browse...' button, the text 'No file selected.', and an 'Upload' button.

### Delete the custom wallpaper

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

You have to upload it anew if you want use it again.

## About a custom wallpaper

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

You can only store one custom wallpaper on the video system at a time; a new custom wallpaper overwrites the old one.

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

- The large clock
- The list of upcoming meetings

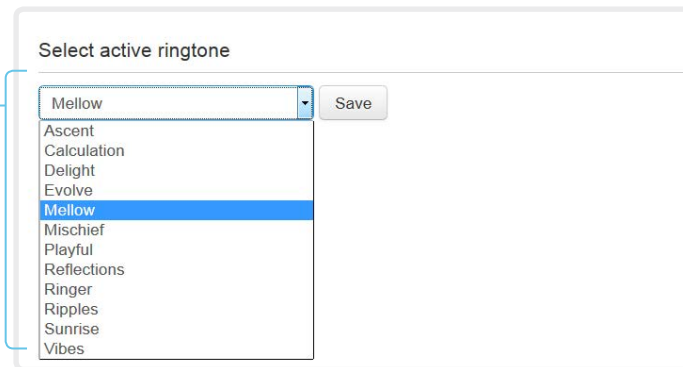


## Choose a ringtone and set the ringtone volume

Sign in to the web interface, and navigate to [Setup > 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. Use the web interface to chose 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 [Setup > Local Contacts](#).

### 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.

The 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 contact's name followed by [Edit contact](#).

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

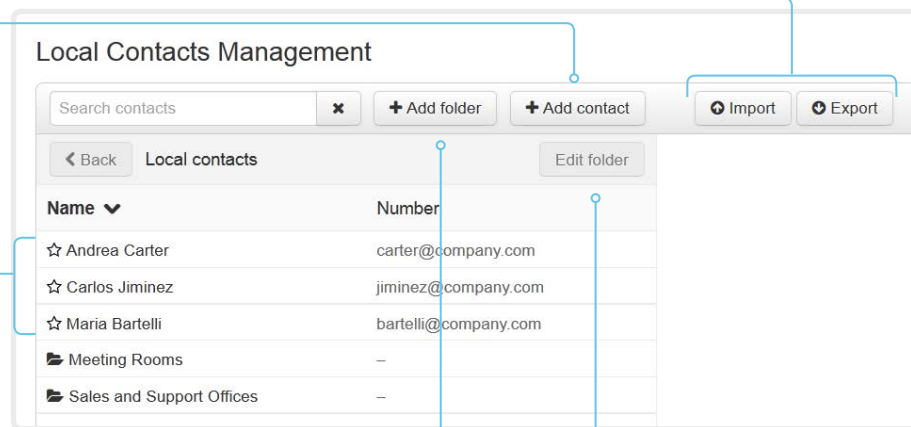
Choose a folder in the folder drop down list in order to store the contact in a sub-folder.

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.

**Remote control and on-screen menu:** Select [Call > Directory > Local contacts](#). The local contacts are listed alphabetically without regard to the folder hierarchy.

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

## Favorites list

The Favorites list is only available in the on-screen menu. It is not available on the Touch controller or the web interface.

Select [Call > Favorites](#) to find the list. You can add both Local contacts and other Directory entries to the Favorites list.

Also, a directory entry that is marked as a favorite is automatically copied to the Local contacts folder.

## Add a contact to the Favorites list

**Remote control and on-screen menu:** Navigate to the contact, and then [⋮](#). Click [Mark as Favorite](#).

**Web interface:** Navigate to [Setup > Local Contacts](#). Click the star next to the contact.



## Chapter 3

# Peripherals

## 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 2)

In order to use Touch 10 as user interface for SX10, Touch 10 must be paired to the video system via the network (LAN). This is referred to as remote pairing.

### Connect Touch 10 to the video system via the network (LAN)

Connect Touch 10 and the video system 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 a room system](#) screen appears, note the following:

- A list of video systems signalling that they are available for pairing will show up on the screen. Tap the name of the system you want to pair with.

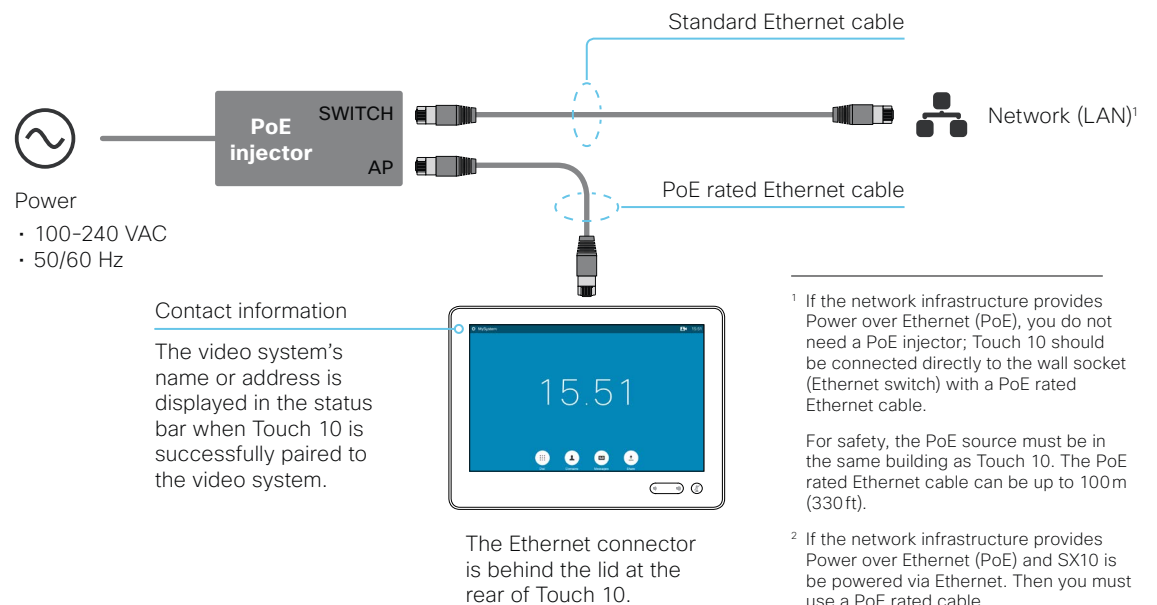
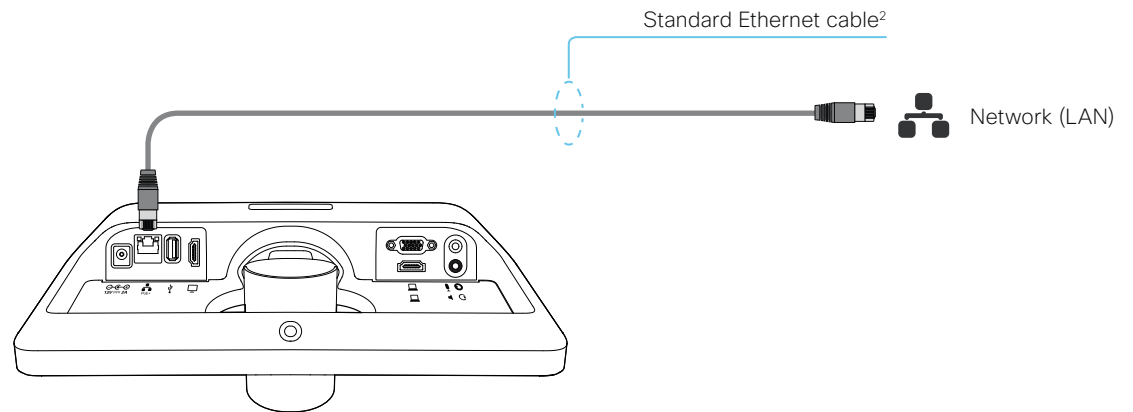
Note that the following must be fulfilled for a video system to show up in the list:

- The video system and Touch 10 must be on the same subnet.
- The video system must have been restarted within the last 10 minutes. If the video system does not appear in the list, try restarting it.
- If the video system does not appear in the list of available systems, enter its IP address or hostname in the input field. Tap [Enter](#) or [Continue](#).
- You have to log in with username and passphrase for the pairing process to commence. Tap [Login](#) or [Continue](#).

A user with the USER role is sufficient; you do not need the ADMIN role to perform this task.

Read more about how to create a user account and assign a role to it in the [User administration](#) chapter.

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



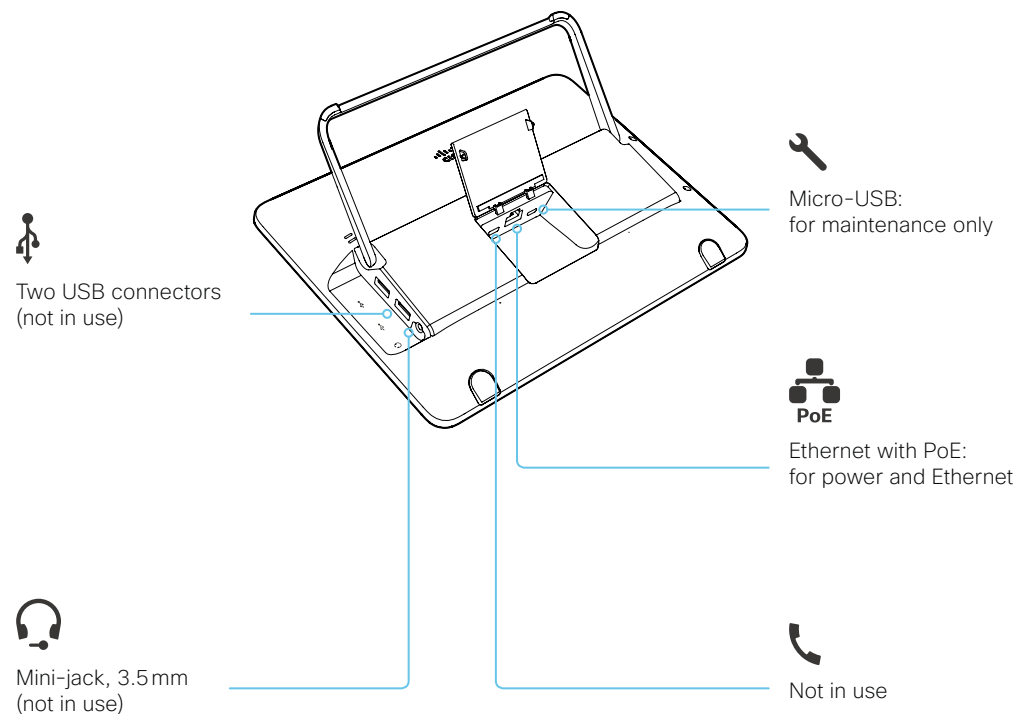
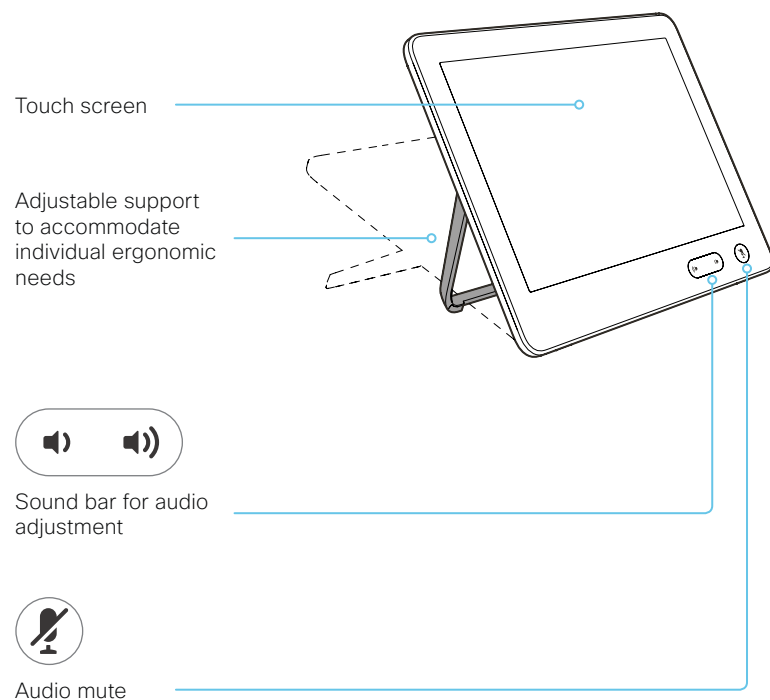
<sup>1</sup> If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

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).

<sup>2</sup> If the network infrastructure provides Power over Ethernet (PoE) and SX10 is be powered via Ethernet. Then you must use a PoE rated cable.

## Connect the Touch 10 controller (page 2 of 2)

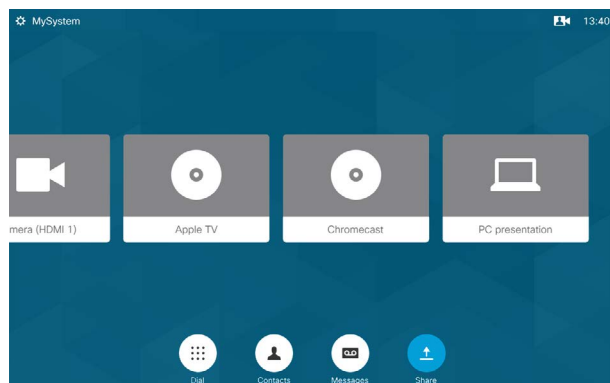
### Touch 10 physical interface



## Extend the number of input sources

You can customize our touch user interfaces to include input sources that are connected to a third-party external video switch.

The sources will appear and behave as any other video source that is connected directly to the video system.



User interface with example external input sources

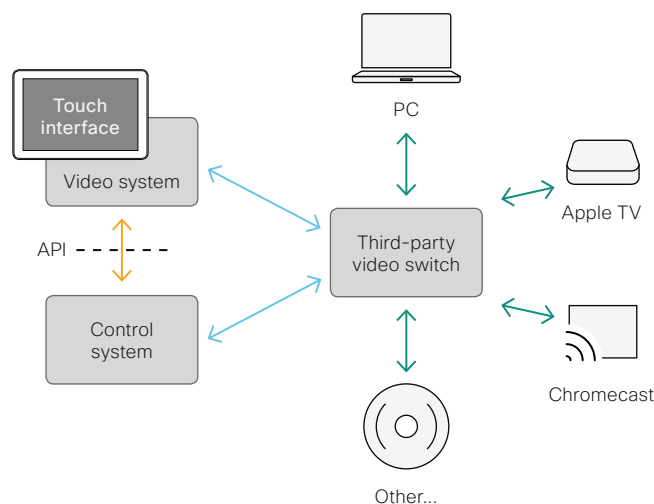
Consult the *In-Room Control guide* for full details about how to extend the user interface, and how to use the video system's API to set it up. Go to:

► <http://www.cisco.com/go/in-room-control-docs>

## Architecture

You need a Cisco video system with a touch interface, a third-party control system, for example Crestron or AMX, and a third-party video switch. It is the control system, not the video system, that controls the video switch.

When you program the control system you must use the video system's API (events and commands)\* in order to connect with the video switch and the controls on the touch interface. This way you can synchronize what is shown and done on the user interface with the actual state of the input sources.



\* You need a user that holds the ROOMCONTROL or ADMIN user roles in order to access the API commands that you need when programming the control system.



## Chapter 4

# Maintenance



## Upgrade the system software (page 1 of 2)

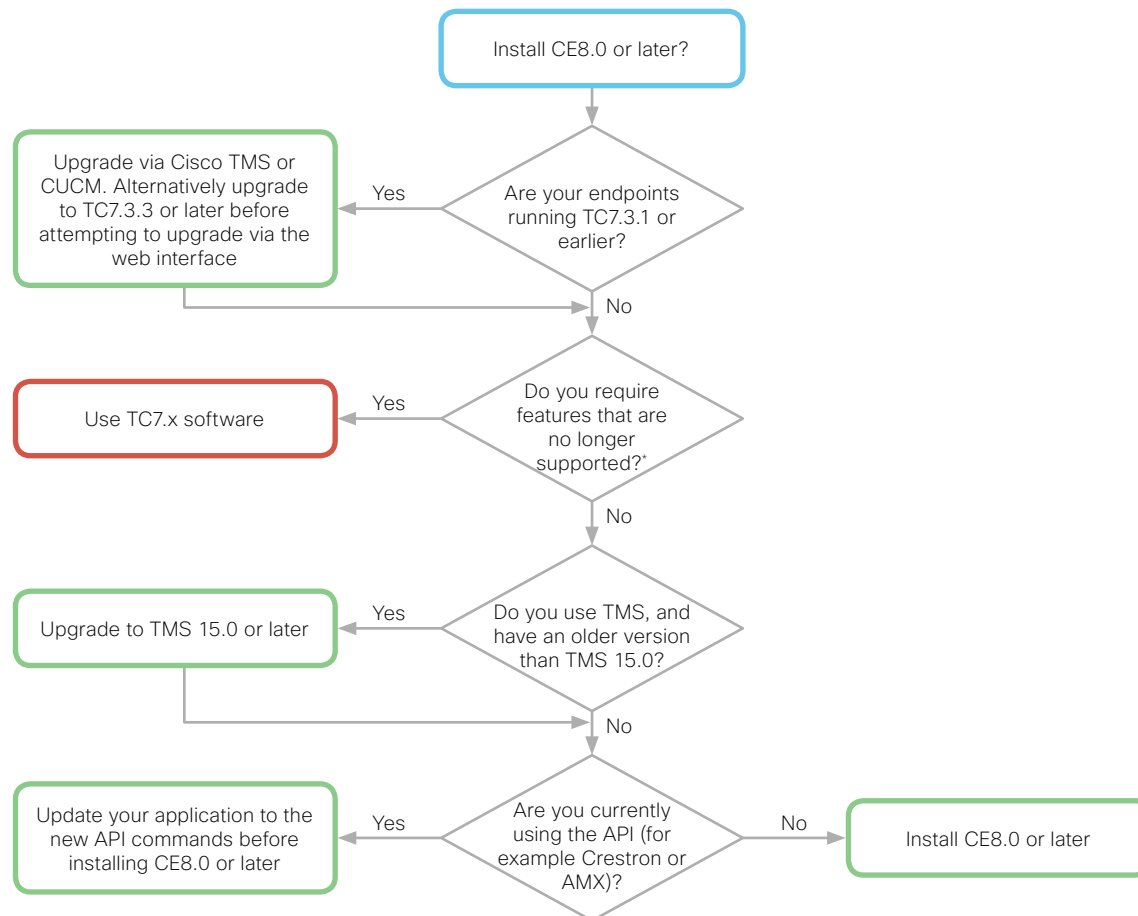
### About upgrading from TC to CE software

CE8.x is the evolution of TC7.x software. CE8.x 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.x 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 or later. 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.x can leave you with a non-functioning deployment that requires you to downgrade.



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

- CTMS conferencing
- MediaNet
- 4:3 video resolutions

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 "s52030ce8\_3\_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 CE8.3.x.

### Install new software

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

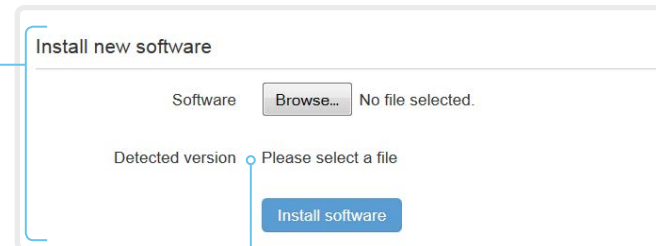
1. Click [Browse...](#) and find the .pkg file that contains the new software.

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.



### Check software version

The software version shows here when you have selected a file.

## Add option keys

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

You see a list of all option keys, also the ones that are not installed on your video system.

Contact your Cisco representative for information about how to get option keys for the uninstalled options.

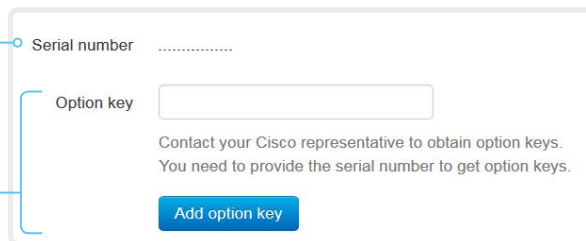
### The video system's serial number

You need the video system's serial number when ordering an option key.

### Add an option key

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

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



Serial number .....

Option key

Contact your Cisco representative to obtain option keys.  
You need to provide the serial number to get option keys.

[Add option key](#)

## 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.

## System status

### System information overview

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

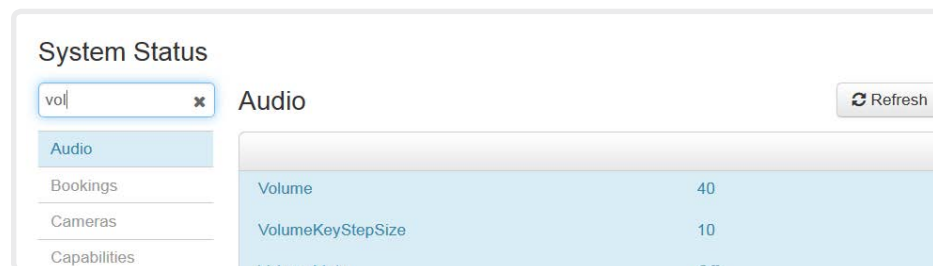
This page shows the product type, system name and basic information about the hardware, software, installed options and network address. Registration status for the video networks (SIP and H.323) is included, as well as the number/URI to use when making a call to the system.

### Detailed system status

Sign in to the web interface, and navigate to [Setup > 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.

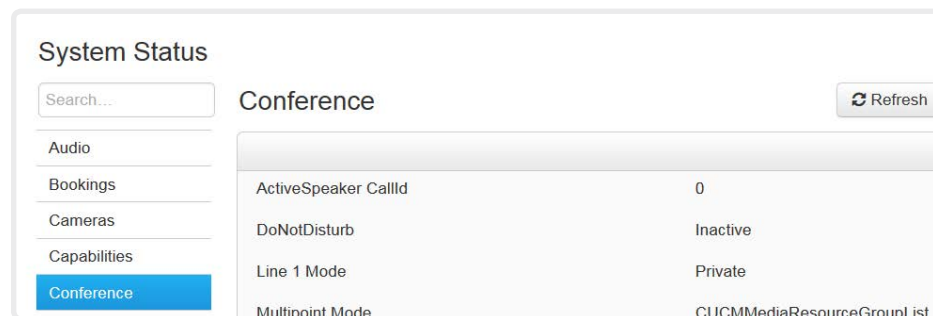


The screenshot shows the 'System Status' page with a search bar containing 'vol'. The left sidebar has a menu with 'Audio' selected. The main content area displays a table of audio-related status items.

Audio	
Volume	40
VolumeKeyStepSize	10

### 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' page with a search bar. The left sidebar has a menu with 'Conference' selected. The main content area displays a table of conference-related status items.

Conference	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private
Multinoint Mode	CUCMMediaResourceGroup list

\* 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 [Maintenance > Diagnostics](#).

The diagnostics page lists the status for some common sources of errors\*.

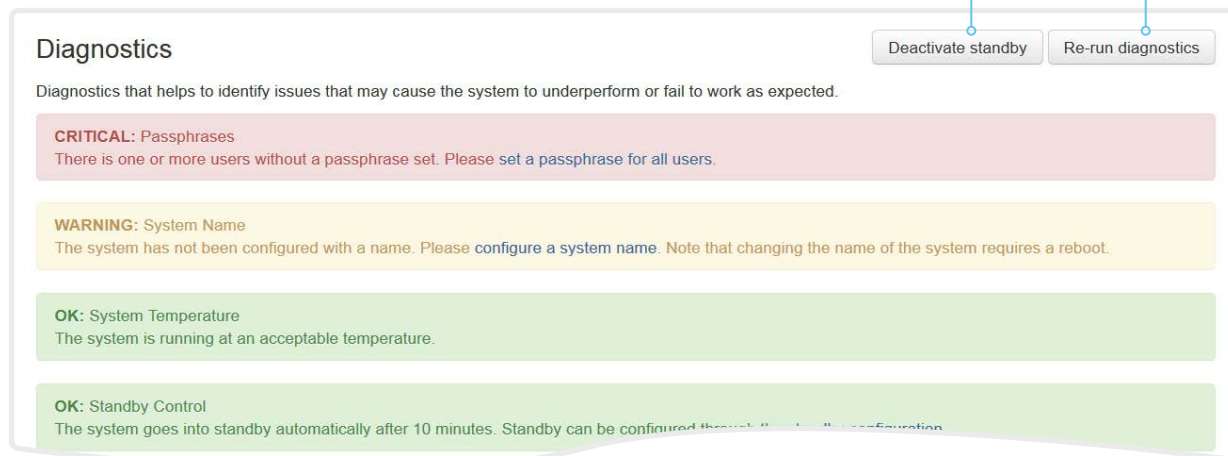
Errors and critical issues are clearly marked in red color; warnings are yellow.

### Run diagnostics

Click [Re-run diagnostics](#) to ensure that the list is up to date.

### Leave standby mode

Click [Deactivate standby](#) to wake up a video system that is in standby mode.



**Diagnostics**

Diagnostics that helps to identify issues that may cause the 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.

Deactivate standby Re-run diagnostics

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

## Download log files

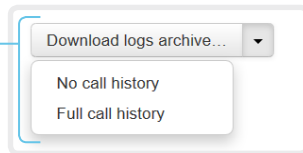
Sign in to the web interface and navigate to  
[Maintenance](#) > [System Logs](#).

### 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.

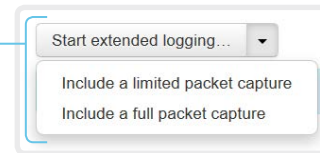
### Start extended logging

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.



## 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.




### Refresh a log file list

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

## 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.

The system does not have an active Remote Support User.

Create user

Delete user

This user is valid until  
2015-11-11 08:35:06

#### Token

```
bgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5z1+b
TQek1PaSpsQJNEMfzThgbvK4J7pgOyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
e9CpAoRNg+mZMqEG1lsswKPZ7HYulvyVTH/XuPzU7Nues
9pwzLc8BFgBt1xV0fKeoeOmMX+it1EcamlN4lnXl8cgOt
yPSXiFWLdKAJsQHJQH20PCxxYcnEUYNpAoJiD39edLy4
etY+/SATwBIiohrqF9JLW9FfNEF+IyDlwUmYkPoEirBj7
N3Zvpivlv1Z7+NUalQW9qWTj4Ag==
```

The system has an active Remote Support User.

Create user

Delete user

### 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 reset 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 reset button

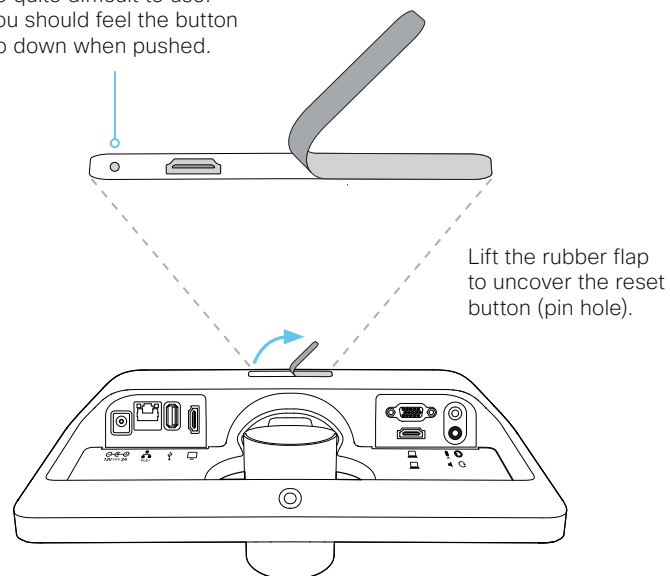
We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.

1. Lift the rubber flap on the back of the unit to uncover the reset button (pin hole).
2. Use the tip of a pen (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.
3. 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.

#### Reset button (pin hole)

The recessed button can be quite difficult to use. You should feel the button go down when pushed.



## 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.

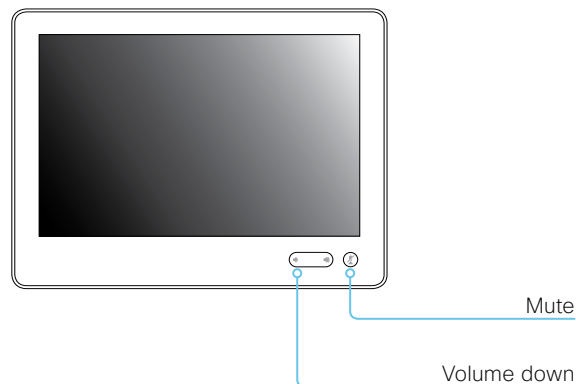


It is not possible to undo a factory reset.

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.

Touch 10 must be paired to the video system anew. When successfully paired it receives a new configuration automatically from the video system.



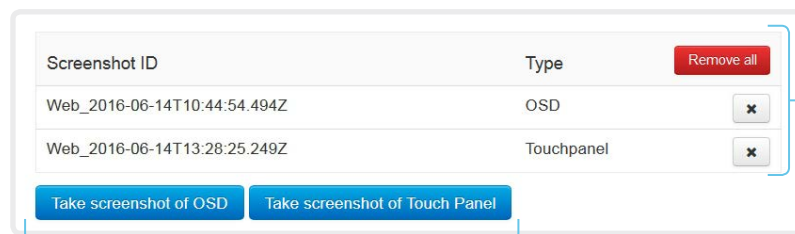
### About pairing and how to connect Touch 10 to the video system

In order to use the Touch 10 controller, Touch 10 must be paired to the codec via LAN (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 [Maintenance > 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 [Setup > 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

1. Select the settings icon (cogwheel) on the home screen, or in the status bar of the Touch controller.
2. Select [System Information](#) with the remote control, or [Settings > System Information](#) on the Touch controller.

<b>Audio settings</b>	<b>75</b>
Audio DefaultVolume	75
Audio Input Microphone [1..2] Mode	76
Audio Input Microphone [2] EchoControl Dereverberation	76
Audio Input Microphone [2] EchoControl Mode	75
Audio Input Microphone [2] EchoControl NoiseReduction	76
Audio Input Microphone [2] Level	76
Audio Microphones Mute Enabled	75
Audio Output Line [1] Delay DelayMs	76
Audio Output Line [1] Delay Mode	76
Audio SoundsAndAlerts RingTone	75
Audio SoundsAndAlerts RingVolume	75
<b>CallHistory settings</b>	<b>77</b>
CallHistory Mode	77
<b>Cameras settings</b>	<b>78</b>
Cameras Camera [1] Backlight DefaultMode	78
Cameras Camera [1] Brightness DefaultLevel	78
Cameras Camera [1] Brightness Mode	78
Cameras Camera [1] Flip	78
Cameras Camera [1] Focus Mode	78
Cameras Camera [1] Mirror	79
Cameras Camera [1] Whitebalance Level	79
Cameras Camera [1] Whitebalance Mode	79
<b>Conference settings</b>	<b>80</b>
Conference ActiveControl Mode	80
Conference AutoAnswer Delay	80
Conference AutoAnswer Mode	80
Conference AutoAnswer Mute	80
Conference CallProtocolIPStack	80
Conference DefaultCall Rate	81
Conference DoNotDisturb DefaultTimeout	81
Conference Encryption Mode	81
Conference FarEndControl Mode	81
Conference FarEndControl SignalCapability	81
Conference MaxReceiveCallRate	81

Conference MaxTotalReceiveCallRate .....	82	Network [1] IEEE8021X Eap Tls .....	90
Conference MaxTotalTransmitCallRate .....	82	Network [1] IEEE8021X Identity .....	90
Conference MaxTransmitCallRate .....	82	Network [1] IEEE8021X Mode .....	89
Conference MicUnmuteOnDisconnect Mode .....	82	Network [1] IEEE8021X Password .....	90
Conference Presentation OnPlacedOnHold .....	82	Network [1] IEEE8021X TlsVerify .....	89
Conference VideoBandwidth Mode .....	82	Network [1] IEEE8021X UseClientCertificate .....	89
Conference VideoBandwidth PresentationChannel Weight .....	83	Network [1] IPStack .....	91
<b>FacilityService settings .....</b>	<b>84</b>	Network [1] IPv4 Address .....	91
FacilityService Service [1..5] CallType .....	84	Network [1] IPv4 Assignment .....	91
FacilityService Service [1..5] Name .....	84	Network [1] IPv4 Gateway .....	91
FacilityService Service [1..5] Number .....	84	Network [1] IPv4 SubnetMask .....	91
FacilityService Service [1..5] Type .....	84	Network [1] IPv6 Address .....	92
<b>H323 settings .....</b>	<b>85</b>	Network [1] IPv6 Assignment .....	92
H323 Authentication LoginName .....	85	Network [1] IPv6 DHCPOptions .....	92
H323 Authentication Mode .....	85	Network [1] IPv6 Gateway .....	92
H323 Authentication Password .....	85	Network [1] MTU .....	92
H323 CallSetup Mode .....	85	Network [1] QoS Diffserv Audio .....	93
H323 Encryption KeySize .....	86	Network [1] QoS Diffserv Data .....	93
H323 Gatekeeper Address .....	86	Network [1] QoS Diffserv ICMPv6 .....	94
H323 H323Alias E164 .....	86	Network [1] QoS Diffserv NTP .....	94
H323 H323Alias ID .....	86	Network [1] QoS Diffserv Signalling .....	93
H323 NAT Address .....	87	Network [1] QoS Diffserv Video .....	93
H323 NAT Mode .....	86	Network [1] QoS Mode .....	92
H323 PortAllocation .....	87	Network [1] RemoteAccess Allow .....	94
<b>Logging settings .....</b>	<b>88</b>	Network [1] Speed .....	94
Logging External Mode .....	88	Network [1] TrafficControl Mode .....	95
Logging External Protocol .....	88	Network [1] VLAN Voice Mode .....	95
Logging External Server Address .....	88	Network [1] VLAN Voice VlanId .....	95
Logging External Server Port .....	88	<b>NetworkServices settings .....</b>	<b>96</b>
Logging Mode .....	88	NetworkServices CDP Mode .....	96
<b>Network settings .....</b>	<b>89</b>	NetworkServices H323 Mode .....	96
Network [1] DNS Domain Name .....	89	NetworkServices HTTP Mode .....	96
Network [1] DNS Server [1..3] Address .....	89	NetworkServices HTTPS OCSP Mode .....	97
Network [1] IEEE8021X AnonymousIdentity .....	90	NetworkServices HTTPS OCSP URL .....	97
Network [1] IEEE8021X Eap Md5 .....	90	NetworkServices HTTPS VerifyClientCertificate .....	97
Network [1] IEEE8021X Eap Peap .....	91	NetworkServices HTTPS VerifyServerCertificate .....	96
Network [1] IEEE8021X Eap Tls .....	90	NetworkServices NTP Mode .....	97
		NetworkServices NTP Server [1..3] Address .....	97
		NetworkServices SIP Mode .....	97



NetworkServices SNMP CommunityName .....	98	Proximity Services ContentShare FromClients.....	107
NetworkServices SNMP Host [1..3] Address .....	98	Proximity Services ContentShare ToClients .....	107
NetworkServices SNMP Mode .....	98	<b>RoomReset settings.....</b>	<b>108</b>
NetworkServices SNMP SystemContact.....	98	RoomReset Control.....	108
NetworkServices SNMP SystemLocation .....	98	<b>RTP settings.....</b>	<b>109</b>
NetworkServices SSH AllowPublicKey .....	99	RTP Ports Range Start.....	109
NetworkServices SSH Mode .....	99	RTP Ports Range Stop .....	109
NetworkServices Telnet Mode.....	99	<b>Security settings.....</b>	<b>110</b>
NetworkServices UPnP Mode .....	99	Security Audit Logging Mode .....	110
NetworkServices UPnP Timeout .....	99	Security Audit OnError Action.....	110
NetworkServices WelcomeText.....	100	Security Audit Server Address .....	110
NetworkServices XMLAPI Mode .....	100	Security Audit Server Port .....	111
<b>Peripherals settings .....</b>	<b>101</b>	Security Audit Server PortAssignment.....	111
Peripherals Pairing CiscoTouchPanels RemotePairing .....	101	Security Session InactivityTimeout .....	111
Peripherals Pairing Ultrasound Volume MaxLevel .....	101	Security Session MaxSessionsPerUser.....	111
Peripherals Pairing Ultrasound Volume Mode .....	101	Security Session MaxTotalSessions .....	111
Peripherals Profile Cameras .....	101	Security Session ShowLastLogon .....	111
Peripherals Profile ControlSystems .....	102	<b>SerialPort settings .....</b>	<b>112</b>
Peripherals Profile TouchPanels .....	102	SerialPort LoginRequired .....	112
<b>Phonebook settings .....</b>	<b>103</b>	SerialPort Mode .....	112
Phonebook Server [1] ID .....	103	<b>SIP settings.....</b>	<b>113</b>
Phonebook Server [1] Type.....	103	SIP ANAT.....	113
Phonebook Server [1] URL.....	103	SIP Authentication Password.....	113
<b>Provisioning settings.....</b>	<b>104</b>	SIP Authentication UserName .....	113
Provisioning Connectivity.....	104	SIP DefaultTransport .....	113
Provisioning ExternalManager Address.....	105	SIP DisplayName.....	113
Provisioning ExternalManager AlternateAddress.....	105	SIP Ice DefaultCandidate .....	114
Provisioning ExternalManager Domain .....	106	SIP Ice Mode.....	114
Provisioning ExternalManager Path .....	105	SIP Line .....	114
Provisioning ExternalManager Protocol .....	105	SIP ListenPort .....	114
Provisioning HttpMethod .....	105	SIP Mailbox .....	114
Provisioning LoginName .....	104	SIP PreferredIPMedia.....	115
Provisioning Mode .....	104	SIP PreferredIPSignaling.....	115
Provisioning Password.....	105	SIP Proxy [1..4] Address.....	115
<b>Proximity settings .....</b>	<b>107</b>	SIP TlsVerify .....	115
Proximity Mode.....	107	SIP Turn DiscoverMode .....	115
Proximity Services CallControl .....	107	SIP Turn DropRflx.....	115

SIP Turn Password.....	116	<b>Video settings.....</b>	<b>127</b>
SIP Turn Server.....	116	Video ActiveSpeaker DefaultPIPPosition .....	127
SIP Turn UserName.....	116	Video DefaultLayoutFamily Local.....	127
SIP Type.....	116	Video DefaultLayoutFamily Remote .....	128
SIP URI.....	116	Video DefaultMainSource .....	128
<b>Standby settings.....</b>	<b>117</b>	Video Input Connector [1..3] CameraControl Camerald .....	128
Standby AudioMotionDetection .....	117	Video Input Connector [1..3] CameraControl Mode.....	128
Standby BootAction.....	117	Video Input Connector [1..3] InputSourceType .....	129
Standby Control.....	117	Video Input Connector [1..3] Name .....	129
Standby Delay.....	117	Video Input Connector [1..3] OptimalDefinition Profile.....	129
Standby StandbyAction .....	117	Video Input Connector [1..3] Visibility .....	130
Standby WakeupAction.....	118	Video Input Connector [2..3] PresentationSelection.....	130
<b>SystemUnit settings.....</b>	<b>119</b>	Video Input Connector [2..3] Quality .....	129
SystemUnit Name .....	119	Video Input Connector [2] RGBQuantizationRange.....	130
<b>Time settings.....</b>	<b>120</b>	Video Monitors.....	131
Time DateFormat .....	120	Video Output Connector [1] CEC Mode .....	131
Time TimeFormat.....	120	Video Output Connector [1] OverscanLevel.....	131
Time Zone.....	121	Video Output Connector [1] Resolution.....	131
<b>UserInterface settings.....</b>	<b>123</b>	Video Output Connector [1] RGBQuantizationRange.....	132
UserInterface ContactInfo Type .....	123	Video Presentation DefaultPIPPosition .....	132
UserInterface KeyTones Mode.....	123	Video Presentation DefaultSource.....	132
UserInterface Language .....	123	Video Selfview Default FullscreenMode .....	133
UserInterface OSD EncryptionIndicator.....	123	Video Selfview Default Mode.....	132
UserInterface OSD Output.....	124	Video Selfview Default PIPPosition.....	133
UserInterface UserPreferences .....	124	Video Selfview OnCall Duration .....	133
UserInterface Wallpaper .....	124	Video Selfview OnCall Mode .....	133
<b>UserManagement settings.....</b>	<b>125</b>	<b>Experimental settings .....</b>	<b>134</b>
UserManagement LDAP Admin Filter .....	126		
UserManagement LDAP Admin Group .....	126		
UserManagement LDAP Attribute.....	126		
UserManagement LDAP Encryption .....	125		
UserManagement LDAP MinimumTLSVersion.....	125		
UserManagement LDAP Mode .....	125		
UserManagement LDAP Server Address .....	125		
UserManagement LDAP Server Port.....	125		
UserManagement LDAP VerifyServerCertificate.....	126		

## 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 or remote control 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: ADMIN, 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: ADMIN, 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: ADMIN, 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 Microphone [2] EchoControl Mode

The echo canceller continuously adjusts itself to the audio characteristics of the room, and compensates for any changes it detects in the audio environment. If the changes in the audio conditions are 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: Turn off the echo control. Recommended if external echo cancellation or playback equipment is used.

On: Turn on the echo control. Recommended, in general, to prevent the far end from hearing their own audio. Once selected, echo cancellation is active at all times.

## Audio Input Microphone [2] EchoControl NoiseReduction

The system has built-in noise reduction, which reduces stationary background noise, for example noise from air-conditioning systems, cooling fans etc. In addition, a high pass filter (Humfilter) reduces very low frequency noise. Noise reduction requires that Audio Input Microphone [n] EchoControl Mode is enabled.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Turn off the noise reduction.

On: Turn on the noise reduction. Recommended in the presence of low frequency noise.

## Audio Input Microphone [2] EchoControl Dereverberation

The system has built-in signal processing to reduce the effect of room reverberation. Dereverberation requires that Audio Input Microphone [n] EchoControl Mode is enabled.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

## Audio Input Microphone [2] Level

Define the audio level of the Microphone input connector.

Requires user role: ADMIN

Default value: 17

Value space: Integer (0..24)

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

## Audio Input Microphone [1..2] Mode

Disable or enable audio on the microphone connector. Note that Microphone [1] is the video system's internal microphone.

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 Output Line [1] Delay DelayMs

To obtain lip-synchronization, you can configure each audio line output with an extra delay that compensates for delay in other connected devices, for example TVs and external loudspeakers. The delay that you set here is either fixed or relative to the delay on the HDMI output, as defined in the Audio Output Line [n] Delay Mode setting.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..290)

The delay in milliseconds.

## Audio Output Line [1] Delay Mode

You may add extra delay to an audio line output with the Audio Output Line [n] Delay DelayMs setting. The extra delay added is either a fixed number of milliseconds, or a number of milliseconds relative to the detected delay on the HDMI output (typically introduced by the connected TV).

Requires user role: ADMIN

Default value: RelativeToHDMI

Value space: Fixed/RelativeToHDMI

Fixed: Any extra delay (DelayMs) added to the output, will be a fixed number of millisecond.

RelativeToHDMI: Any extra delay (DelayMs) added to the output, will be relative to the detected delay on the HDMI output. The actual delay is HDMI-delay + DelayMs. The Audio Output Connectors Line [n] DelayMs status reports the actual delay.

## 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] 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: ADMIN, 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] Brightness Mode

Define the camera brightness mode.

Requires user role: ADMIN, 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] Brightness DefaultLevel

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

Requires user role: ADMIN, USER

Default value: 20

Value space: Integer (1..31)

The brightness level.

### Cameras Camera [1] 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: ADMIN, USER

Default value: Auto

Value space: Auto

Auto: If the camera detects that it is mounted upside down, the image is automatically flipped.

### Cameras Camera [1] Focus Mode

Define the camera focus mode.

Requires user role: ADMIN, 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] 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: ADMIN, 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] Whitebalance Mode

Define the camera white balance mode.

Requires user role: ADMIN, 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] Whitebalance Level

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

Requires user role: ADMIN, USER

Default value: 1

Value space: Integer (1..16)

The white balance level.

## Conference settings

### Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server or Cisco Meeting 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, Cisco Media Server (CMS) version 2.1 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 pressing the OK key or the green Call key on the remote control, or 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).

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 Rate

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

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

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. The default value is 60 minutes.

Requires user role: ADMIN

Default value: 60

Value space: Integer (1..1440)

The number of minutes (maximum 1440 minutes = 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: 3072

Value space: Integer (64..3072)

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: 3072

Value space: Integer (64..3072)

The maximum transmitt call rate (kbps).

## Conference MaxTotalReceiveCallRate

Define the maximum overall receive bit rate allowed. This product does not support multiple simultaneous calls, so the total receive call rate will be the same as the receive bit rate for one call (ref. Conference MaxReceiveCallRate setting).

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

The maximum receive call rate (kbps).

## Conference MaxTotalTransmitCallRate

Define the maximum overall transmit bit rate allowed. This product does not support multiple simultaneous calls, so the total transmit call rate will be the same as the transmit bit rate for one call (ref. Conference MaxTransmitCallRate setting).

Requires user role: ADMIN

Default value: 3072

Value space: Integer (64..3072)

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 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 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..9)

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. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Default value: Helpdesk

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

Catering: Select this option for catering services.

Concierge: Select this option for concierge services.

Emergency: Select this option for emergency services.

Helpdesk: Select this option for helpdesk services.

Security: Select this option for security services.

Transportation: Select this option for transportation services.

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

### 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. The facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Default value: Service 1: "Live Support" Other services: ""

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. The facility services are not available when using the remote control and on-screen menu.

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. Facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Default value: Video

Value space: Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.

## 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: Min1024bit

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 External Mode

Determine whether or not to use a remote syslog server for logging.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable logging to a remote syslog server.

On: Enable logging to a remote syslog server.

### Logging External Protocol

Determine which protocol to use toward the remote logging server. You can use either the syslog protocol over TLS (Transport Layer Security), or the syslog protocol in plaintext. For details about the syslog protocol, see RFC 5424.

Requires user role: ADMIN

Default value: SyslogTLS

Value space: Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

### Logging External Server Address

The address of the remote syslog server.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

### Logging External Server Port

The port that the remote syslog server listens for messages on. If set to 0, which is the default, the video system will use the standard syslog port. The standard syslog port is 514 for syslog, and 6514 for syslog over TLS.

Requires user role: ADMIN

Default value: 514

Value space: Integer (0..65535)

The number of the port that the remote syslog server is using. 0 means that the video system uses the standard syslog port.

### 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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

Default value: ""

Value space: String (0, 64)

A valid IPv6 address including a network mask. Example: 2001:DB8::/48

## 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, USER

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, USER

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) size. The MTU size must be supported by your network infrastructure. The minimum size is 576 for IPv4 and 1280 for IPv6.

Requires user role: ADMIN, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

Default value: ""

Value space: String (0, 255)

A valid IPv4 address or IPv6 address.

## Network [1] Speed

Define the Ethernet link speed. We recommend not to change from the default value, which negotiates with the network to set the speed automatically. If you do not use autonegotiation, make sure that the speed you choose is supported by the closest switch in your network infrastructure.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/10half/10full/100half/100full

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.

## Network [1] TrafficControl Mode

Define the network traffic control mode to decide how to control the video packets transmission speed.

Requires user role: ADMIN, USER

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, USER

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, USER

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: Off

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, 255)

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, 255)

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 controller) as user interface for the video system, Touch 10 must be paired to the video system via the network (LAN). This 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..70)

Select a value in the specified range. If set to 0, the ultrasound is switched off.

### Peripherals Profile Cameras

Define the number of cameras 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 cameras does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN

Default value: Minimum1

Value space: NotSet/Minimum1/0/1/2/3/4/5/6/7

NotSet: No camera check is performed.

Minimum1: At least one camera should be connected to the video system.

0-7: Select the number of cameras that are expected to be connected to the video system.

## Peripherals Profile ControlSystems

Define if a third-party control system, for example Crestron or AMX, is expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected control systems does not match this setting, the diagnostics service will report it as an inconsistency. Note that only one third-party control system is supported.

If set to 1, the control system must send heart beats to the video system using xCommand Peripherals Pair and HeartBeat commands. Failing to do so will cause the in-room control extensions to show a warning that the video system has lost connectivity to the control system.

Requires user role: ADMIN

Default value: NotSet

Value space: 1/NotSet

1: One third-party control system should be connected to the video system.

NotSet: No check for a third-party control system is performed.

## 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/CUCM/Spark/TMS/VCS

Off: Do not use a phonebook.

CUCM: The phonebook is located on the Cisco Unified Communications Manager.

Spark: The phonebook is located on Spark.

TMS: The phonebook is located on the Cisco TelePresence Management Suite server.

VCS: The phonebook is located on the Cisco TelePresence Video Communication Server.

### 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, USER

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, USER

Default value: Auto

Value space: Off/Auto/CUCM/Edge/Spark/TMS/VCS

Off: The video system is not configured by a provisioning system.

Auto: Automatically select the provisioning 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.

Spark: Push configurations to the video system from Spark.

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).

### 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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

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, USER

Default value: Enabled

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, USER

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.

## RoomReset settings

### RoomReset Control

Not applicable.

## 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, 255)

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 from a web, Telnet, or SSH session.

Restart the system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10000)

Set the inactivity timeout (minutes); or select 0 when inactivity should not enforce automatic logout.

## Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user. 0, which is the default value, means no hard limit. Sessions consume resources, so there will be some limitation, but this may vary based on different criteria.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..100)

The maximum number of sessions per user. 0 means no hard limit.

## Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total. 0, which is the default value, means no hard limit. Sessions consume resources, so there will be some limitation, but this may vary based on different criteria.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..100)

The maximum number of sessions in total. 0 means no hard limit.

## 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 (connection via Micro USB to USB cable). The serial port uses 115200 bps, 8 data bits, no parity and 1 stop bit.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the serial port.

On: Enable the serial port.

### 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, 550)

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 video systems can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the video systems.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

Auto: ICE is enabled if a TURN server is provided, otherwise ICE is disabled.

Off: ICE is disabled.

On: ICE is enabled.

## SIP Ice DefaultCandidate

The ICE protocol needs some time to reach a conclusion about which media route to use (up to the first 5 seconds of a call). During this period media for the video system will be sent to the Default Candidate as defined in this setting.

Requires user role: ADMIN

Default value: Host

Value space: Host/Rflx/Relay

Host: Send media to the video system's private IP address.

Rflx: Send media to the video system's public IP address, as seen by the TURN server.

Relay: Send media to the IP address and port allocated on the TURN server.

## 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 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 AudioMotionDetection

The video system is able to automatically discover that people are in its proximity. Given that this feature is switched on, the video system wakes up from standby when someone is detected.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Detection of people in proximity of the video system is switched off.

On: Detection of people in proximity of the video system is switched on.

### 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, USER

Default value: RestoreCameraPosition

Value space: None/DefaultCameraPosition/RestoreCameraPosition

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, USER

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: ADMIN, 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: ADMIN, 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: ADMIN, 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\_Nelson, 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/Montevidео, 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/DumontD'Urville, 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/Barnaul, 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/Tomsk, 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/Astrakhan, 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/Kirov, 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/Ulyanovsk, 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/SipUri/SystemName/DisplayName

Auto: Show the address which another system can dial to reach this system. The address depends on the system registration.

None: Do not show any contact information.

IPv4: Show the system's IPv4 address.

IPv6: Show the system's IPv6 address.

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 pressing a key on the remote control, or when typing text or numbers on the Touch controller.

Requires user role: ADMIN, 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.

Requires user role: ADMIN, USER

Default value: English

Value space: Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

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 menus, information and indicators (OSD) should be displayed. The system supports only one monitor, so this value is fixed and cannot be changed.

Requires user role: ADMIN

Default value: 1

Value space: 1

## 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 4 MByte. When you use a custom wallpaper, the clock and the list of upcoming meetings are removed from the main display

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/Custom/None

Auto: Use the default wallpaper.

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.

## UserManagement settings

### UserManagement LDAP Mode

The video system supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate user names and passwords. Use this setting to configure whether or not to use LDAP authentication. Our implementation is tested for the Microsoft Active Directory (AD) service.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: LDAP authentication is not allowed.

On: Use LDAP authentication.

### UserManagement LDAP Server Address

Set the IP address or hostname of the LDAP server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or hostname.

### UserManagement LDAP Server Port

Set the port to connect to the LDAP server on. If set to 0, use the default for the selected protocol (see the UserManagement LDAP Encryption setting).

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..65535)

The LDAP server port number.

### UserManagement LDAP Encryption

Define how to secure the communication between the video system and the LDAP server. You can override the port number by using the UserManagement LDAP Server Port setting.

Requires user role: ADMIN

Default value: LDAPS

Value space: LDAPS/None/STARTTLS

LDAPS: Connect to the LDAP server on port 636 over TLS (Transport Layer Security).

None: Connect to LDAP server on port 389 with no encryption.

STARTTLS: Connect to LDAP server on port 389, then send STARTTLS to enable TLS encryption.

### UserManagement LDAP MinimumTLSVersion

Set the lowest version of the TLS (Transport Layer Security) protocol that is allowed.

Requires user role: ADMIN

Default value: TLSv1.2

Value space: TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0: Support TLS version 1.0 or higher.

TLSv1.1: Support TLS version 1.1 or higher.

TLSv1.2: Support TLS version 1.2 or higher.

## UserManagement LDAP VerifyServerCertificate

When the video system connects to an LDAP server, the server will identify itself to the video system by presenting its certificate. Use this setting to determine whether or not the video system will verify the server certificate.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The video system will not verify the LDAP server's certificate.

On: The video system must verify that the LDAP server's certificate is signed by a trusted Certificate Authority (CA). The CA must be on the list of trusted CAs that are uploaded to the system in advance. Use the video system's web interface to manage the list of trusted CAs (see more details in the administrator guide).

## UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges. If set, this setting takes precedence over the UserManagement LDAP Admin Group setting.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

Refer to the LDAP specification for the syntax of this string. Example: "(CN=adminuser)"

## UserManagement LDAP Admin Group

Members of this AD (Active Directory) group will be given administrator access. This setting is a shorthand for saying (memberOf:1.2.840.113556.1.4.1941:=<group name>). If UserManagement LDAP Admin Filter is set, this setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The distinguishing name of the AD group. Example: "CN=admin\_group, OU=company groups, DC=company, DC=com"

## UserManagement LDAP Attribute

The attribute used to map to the provided username. If not set, sAMAccountName is used.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The attribute name.

## 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: ADMIN, USER

Default value: 1

Value space: 1

Set the source to be used as the main video source.

## Video Input Connector [1..3] 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 2 (HDMI) and Connector 3 (VGA).

Requires user role: ADMIN

Default value: Connector 1: On Connector 2,3: Off

Value space: Connector 1: Off/On Connector 2,3: Off

Off: Disable camera control.

On: Enable camera control.

## Video Input Connector [1..3] CameraControl CamerId

The camera ID is a unique identifier of the cameras that are connected to the video input.

Requires user role: ADMIN

Default value: 1

Value space: 1

The camera ID is fixed and cannot be changed.



## Video Input Connector [1..3] InputSourceType

Select which type of input source is connected to the video input.

Note that Connector 1 is the system's integrated camera.

Requires user role: ADMIN

Default value: Connector 1: camera Other connectors: PC

Value space: Connector 1: camera Other connectors: PC/camera/desktop/document\_camera/mediaplayer/whiteboard/other

camera: Use this when a camera is connected to the video input.

desktop: Use this when the video system's monitor is the main screen for the PC / laptop that is connected to this input. The Video Input Connector [n] PresentationSelection setting must then also be set to desktop.

document\_camera: Use this when a document camera is connected to the video input.

mediaplayer: Use this when a media player is connected to the video input.

PC: Use this when a computer 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..3] 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 [2..3] 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: 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..3] 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. The resolution must be supported by both the calling and called systems.

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 [2..3] PresentationSelection

Define how the video system will behave when you connect a presentation source to the video input.

If the video system is in standby mode, it will wake up when you connect a presentation source. Sharing the presentation with the far end requires additional action (select Share on the user interface) except when this setting is set to AutoShare.

Requires user role: ADMIN

Default value: OnConnect

Value space: AutoShare/Desktop/Manual/OnConnect

**AutoShare:** While in a call, the content on the video input will automatically be presented to the far end as well as on the local screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). You do not have to select Share on the user interface. If a presentation source is already connected when you make or answer a call, you have to manually select Share on the user interface.

**Desktop:** The content on the video input will be presented on the screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). This applies both when idle and in a call. Also, the content on the video input will stay on the screen when you leave the call, provided that it was the active input at the time of leaving.

**Manual:** The content on the video input will not be presented on the screen until you select Share from the user interface.

**OnConnect:** The content on the video input will be presented on screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). Otherwise, the behavior is the same as in manual mode.

## Video Input Connector [2] 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: Auto

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..3] Visibility

Define the visibility of the video input connector in the menus on the user interface.

Note that Connector 1 is the system's integrated camera, which is not available as a presentation source.

> The default value is Always for Video Input Connector 2 Visibility (the HDMI connector).

> The default value is IfSignal for Video Input Connector 3 Visibility (the VGA connector).

Requires user role: ADMIN

Default value: Connector 1: Never Connector 2: Always Connector 3: OnConnect

Value space: Connector 1: Never Connector 2, 3: 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

Define the monitor layout mode. Note that this video system supports only one monitor, so this value is fixed and cannot be changed.

Requires user role: ADMIN

Default value: Single

Value space: Single

Single: The layout is shown on the video system's monitor.

## Video Output Connector [1] 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] OverscanLevel

Some monitors may not present the entire image that they receive. This means that the outer parts of the image that is sent from the video system may be cut off when displayed on the monitor.

Use this setting to instruct the video system not to use the outer part of the available frame. This part might be cut off by the monitor. Both the video and messages on screen will be scaled in this case.

Requires user role: ADMIN

Default value: None

Value space: None/Medium/High

None: The video system will use all of the output resolution.

Medium: The video system will not use the outer 3% of the output resolution.

High: The video system will not use the outer 6% of the output resolution.

## Video Output Connector [1] Resolution

Define the resolution and refresh rate for the connected screen. This value is fixed and cannot be changed.

Default value: Auto

Value space: Auto

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

## Video Output Connector [1] 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 user interface. 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. It is not relevant when using the user interfaces provided by Cisco.

Requires user role: ADMIN, USER

Default value: 2

Value space: 2

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 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.

CenterRight: 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.

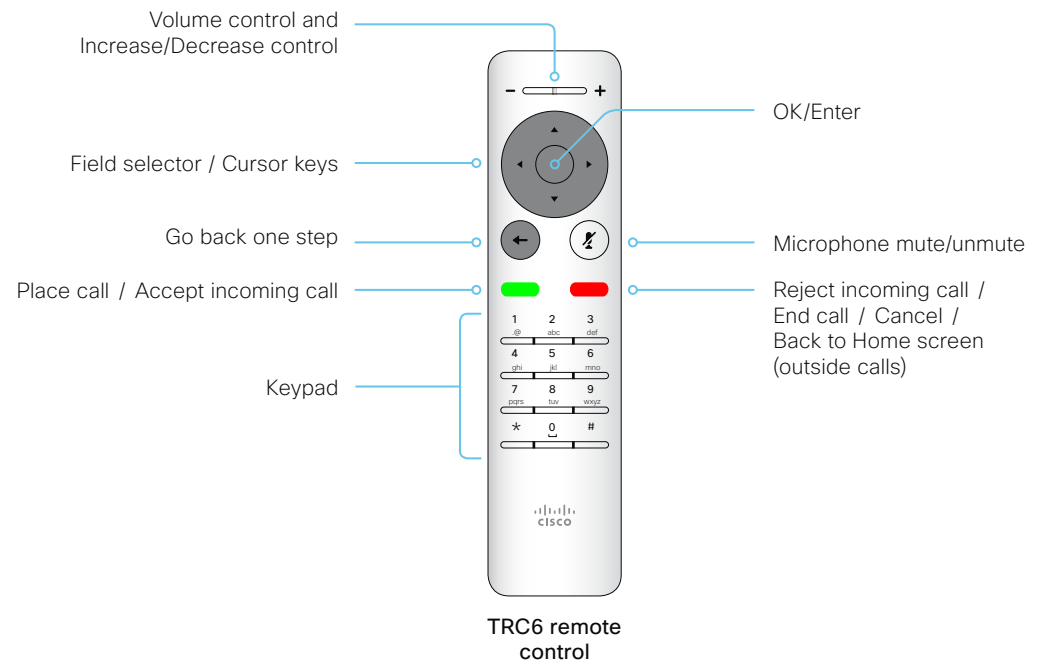
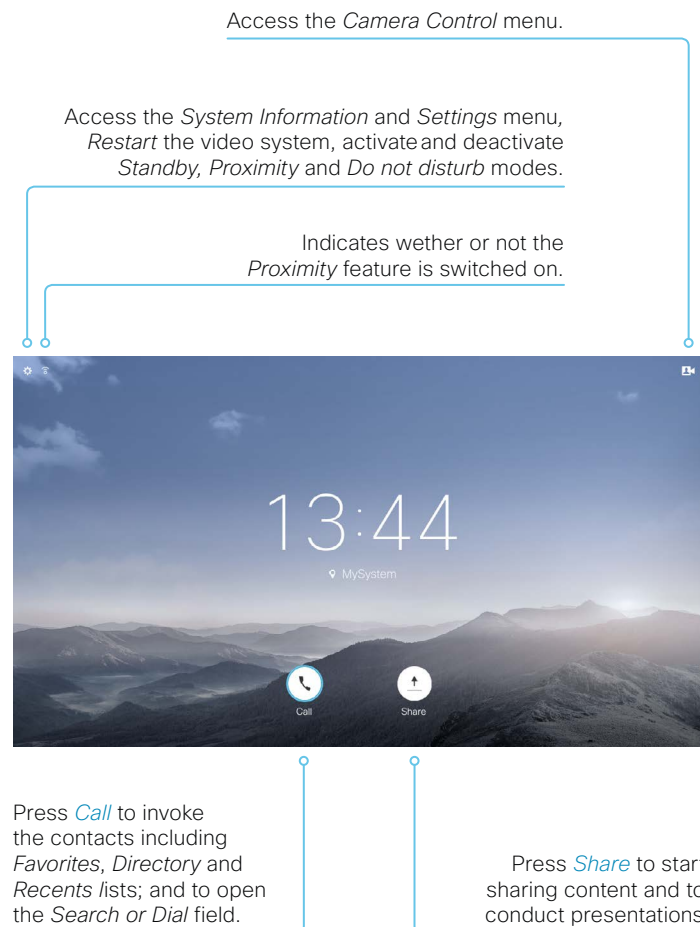


# Appendices

## How to use the remote control and the on-screen user interface

The *User guide* for the video system describes in full detail how to operate the video system using the TRC6 remote control.

The TRC5 remote control is not supported.



### Operating tips

Use the **Cursor** keys to move about the screen. Press **OK/Enter** to open the selected menu field.

Use the **Cancel** key to exit a menu (and return to the *Home* screen), undoing any changes. Use the *Back* key to go just one step back.



## 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 settings icon (cogwheel) to open the *System Information* and *Settings* menu, *Restart* the video system, and activate and deactivate *Standby*, *Proximity* and *Do not disturb* modes.

Entry icon for in-room controls, if available (your system may have a different entry icon).

Tap *?* to contact Help desk, if available.

Tap the *Camera* icon to activate self-view and camera control.

Time of day.

Tap *Share* to start sharing content and to conduct presentations.

Tap *Dial* to invoke the dial pad.

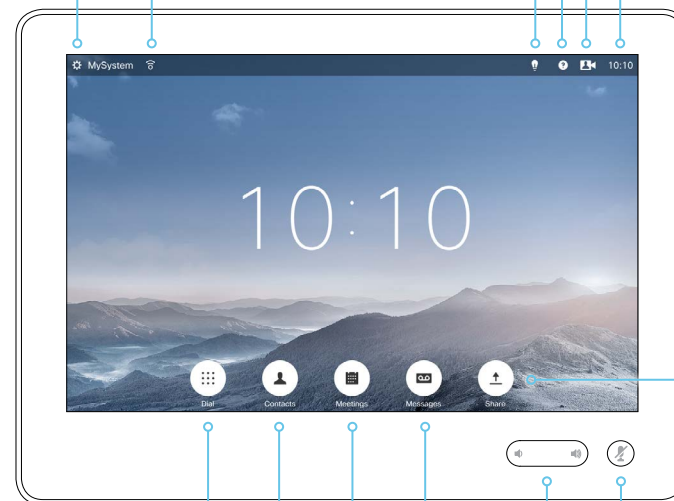
Tap *Contacts* to invoke the list of contacts including *Favorites*, *Directory* and *Recents*.

Tap *Meetings* to invoke a list of upcoming scheduled meetings.

Press the *Microphone* button to mute and unmute microphones.

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.



## Set up remote monitoring

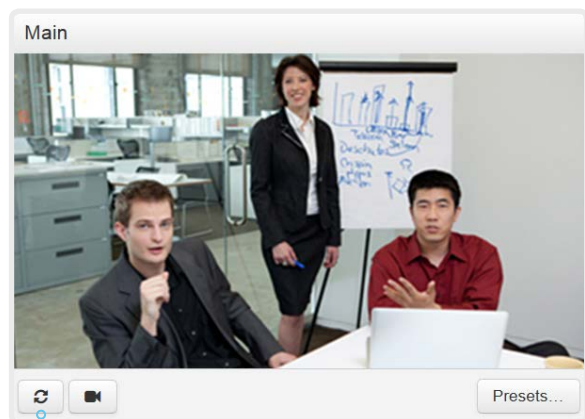
Requirement:

- *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.

If enabled, snapshots are refreshed automatically approximately every 5 seconds.



Automatically refresh snapshots

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 [► Add 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.

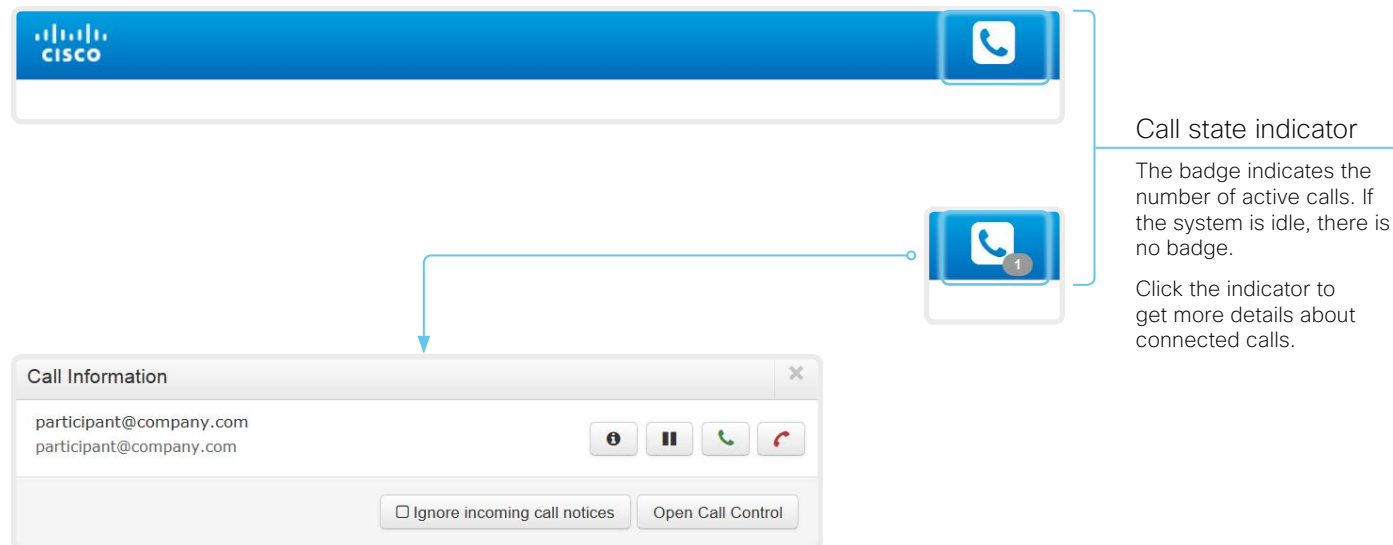
Snapshots appear both when the video system is idle, and when in a call.

### 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



### About the call state indicator

The call state indicator shows whether the system is in a call or not. You may also be notified about incoming calls.

The call state indicator is available on all pages except the [Call Control](#) page.

#### 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.

### 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)

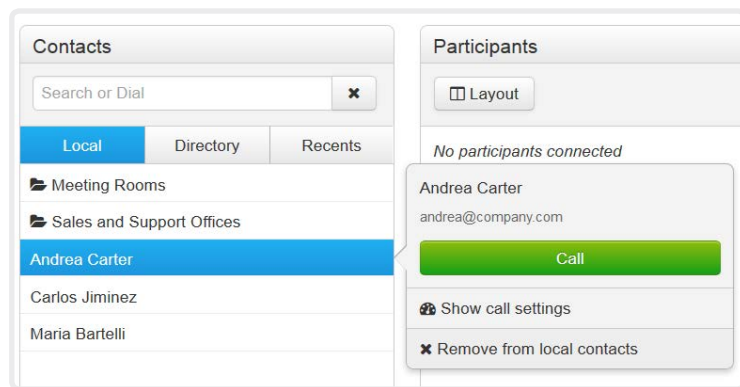
Sign in to the web interface and navigate to [Call Control](#).

### Place a call

 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.

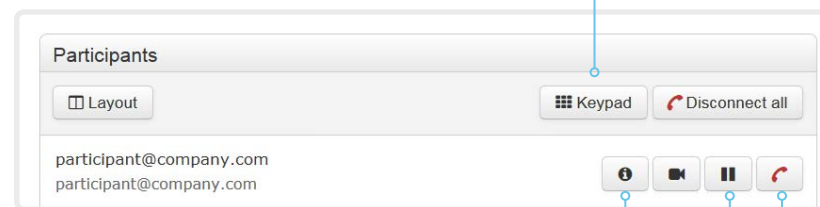
1. Navigate the *Local*, *Directory* or *Recents* lists to find the correct entry; or enter one or more characters in the *Search or Dial* field\*. Click the correct contact name.
2. Click [Call](#) in the contact card.

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.



### Send DTMF tones

Click to open a key pad that you can use if your application requires DTMF (dual-tone multi-frequency) signaling.





### 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, click [Disconnect all](#) or the  button.

\* 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

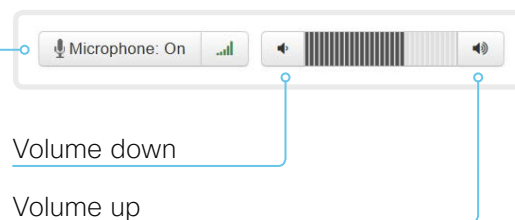
Calling more than one using a conference bridge (CUCM ad hoc conferencing) is not supported from the web interface, even if it is supported by the video system itself.

### 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

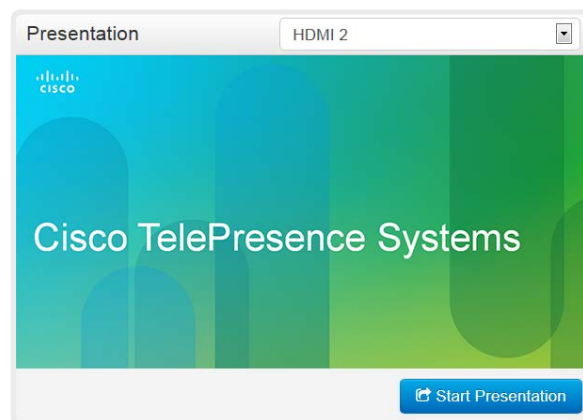
Sign in to the web interface and navigate to [Call Control](#).

### 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

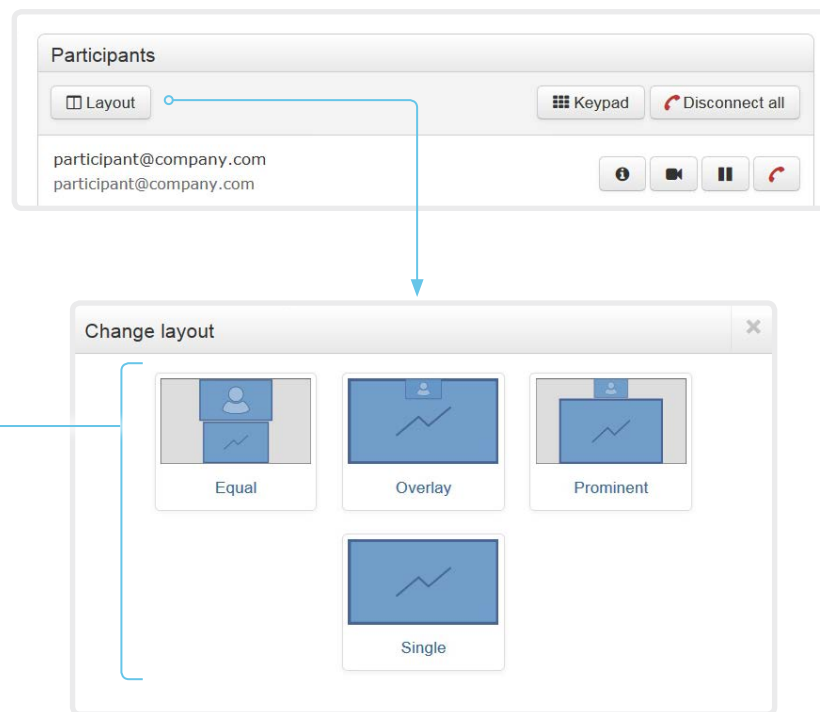
You can connect a presentation source to one of the video inputs of your video system. Most often a PC is used as presentation source, but other options may be available depending on your system setup.

While in a call you can share content with the other participant 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 [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 video and presentation can appear on the screen. Different types of meetings may require different layouts.

## Control a local camera

Sign in to the web interface and navigate to [Call Control](#).

### Prerequisites

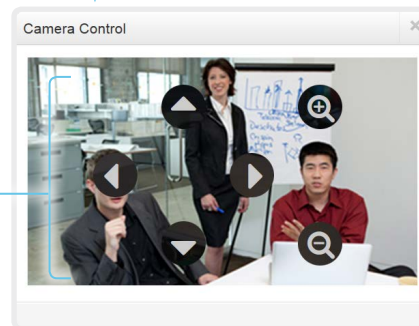
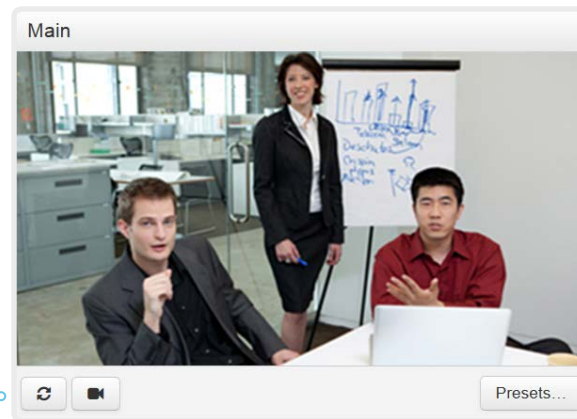
- The [Video > Input > Connector n > CameraControl > Mode](#) setting is switched **On**.
- The camera has pan, tilt or zoom functionality.

### Snapshot area

Shows snapshots of the 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. 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.
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.  
Only relevant controls appear in the window.



### Move the camera to a preset position

1. Click [Presets...](#) to open a list of available presets.  
If no presets are defined, the button is disabled and named *No presets*.
2. Click a preset's name to move the camera to the preset position.
3. Click [OK](#) to close the window.

 You cannot use the web interface to define a preset; you should use the Touch controller.



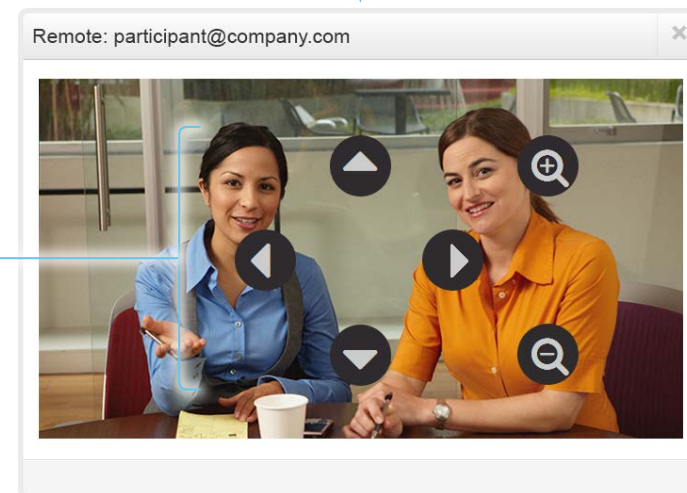
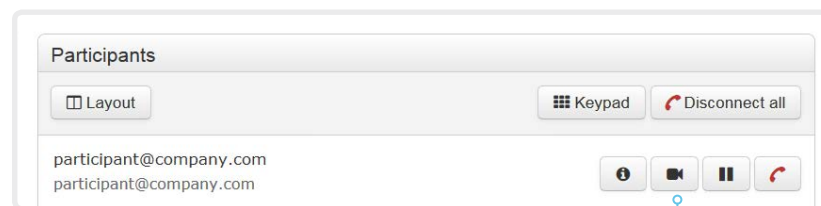
## Control a far end camera

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.

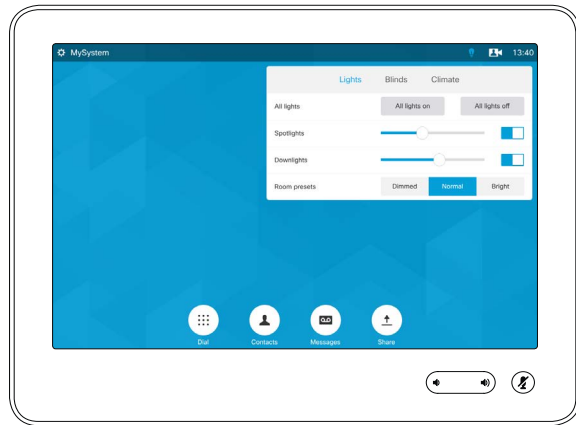
If you are not allowed to control the far end camera, the controls will not appear in the image.

If the call is encrypted, the far end snapshot behind the controls are not displayed.

## Add in-room controls to Touch 10

You can customize our Touch 10 user interface to allow control of peripherals in a meeting room, for example lights and blinds.

This allows for the powerful combination of a control system's functionality and the user-friendly Touch 10 user interface.



Example in-room control panel on Touch 10

Consult the *In-Room Control guide* for full details about how to design an in-room control panel using the In-Room Control editor, and how to use the video system's API to program the in-room controls. Go to:

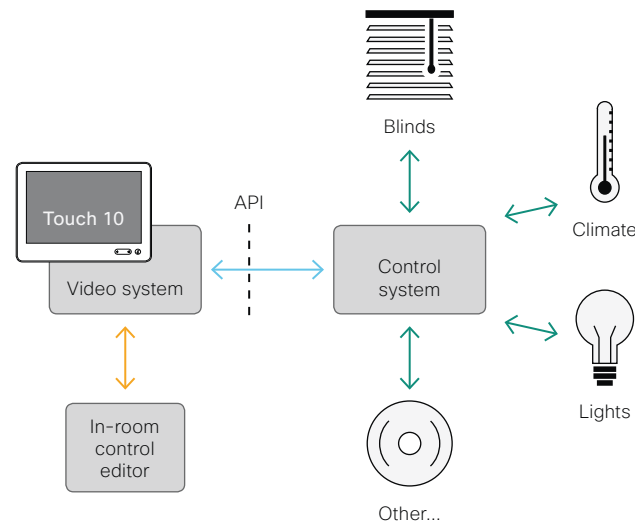
► <http://www.cisco.com/go/in-room-control-docs>

## Architecture

You need a Cisco video system with a Touch controller, and a third-party control system, for example Crestron or AMX, with hardware drivers for the peripherals. It is the control system, not the video system, that controls the peripherals.

When you program the control system you must use the video system's API (events and commands) in order to connect with the controls on the Touch controller.

An easy to use drag-and-drop editor, which you should use to compose the custom in-room control panel, comes free of charge with the video system's software.



In-room control schematics

## The In-Room Control editor

You can use the In-Room Control editor to compose your custom in-room control panels for the Touch controller.

Sign in\* to the web interface, and navigate to [Integration > In-Room Control](#).

- Click [Launch Editor](#) to launch the editor directly from the video system's web interface.

You can push a new in-room control panel to the video system, and see the result immediately on the Touch controller.

- Click [Download Editor](#) to download a stand-alone version that you can use to work offline.

\* You need a user that holds the ROOMCONTROL or ADMIN user roles in order to access the In-Room Control editor and the API commands that you need when programming the control system.

## Manage startup scripts

Sign in to the web interface, and navigate to [Integration > Startup Scripts](#).

### List of startup scripts

You can create one or more startup scripts\*.

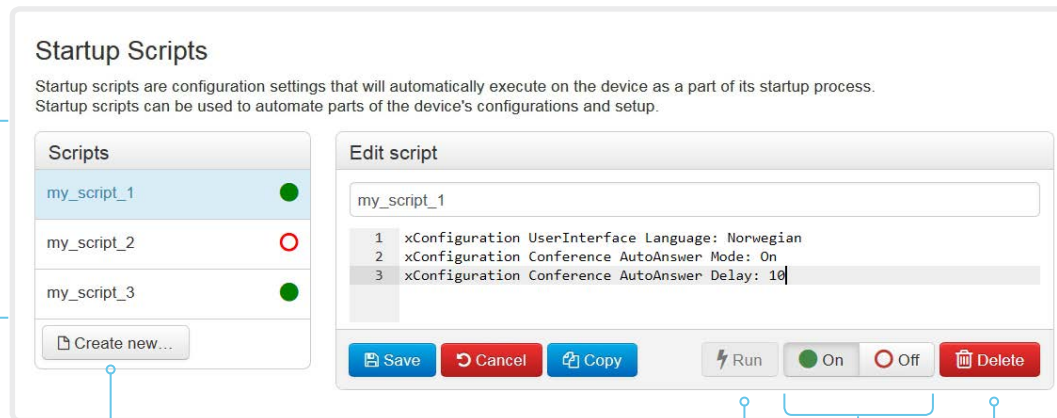
A green dot appears next to an active startup script; a red ring appears next to an inactive startup script.

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.

If you want to use an existing script as a starting point for editing, select that script and click [Copy](#).



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.

## Access the video system's XML files

Sign in to the web interface and navigate to [Integration > Developer 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.

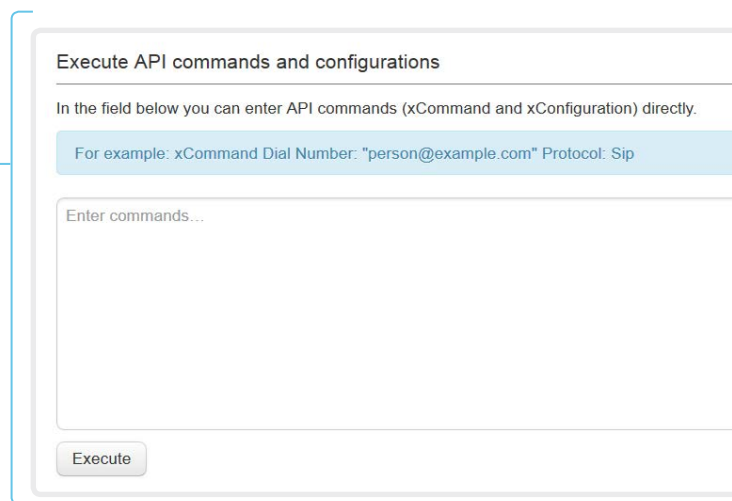
## Execute API commands and configurations from the web interface

Sign in to the web interface and navigate to [Integration > Developer 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.

## Serial interface

Use the micro USB connector for direct communication with the video system. You need a micro USB to USB cable. If the computer doesn't auto-install a serial port driver, you need to install a serial port driver on the computer manually.

Use a terminal emulator (SSH client) to connect to the serial interface. For the most common computer types (PC, MAC) and operating systems, PuTTY or Tera Term will work.

The serial connection can be used without an IP-address, DNS, or a network.

Parameters:

- Baud rate: 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:

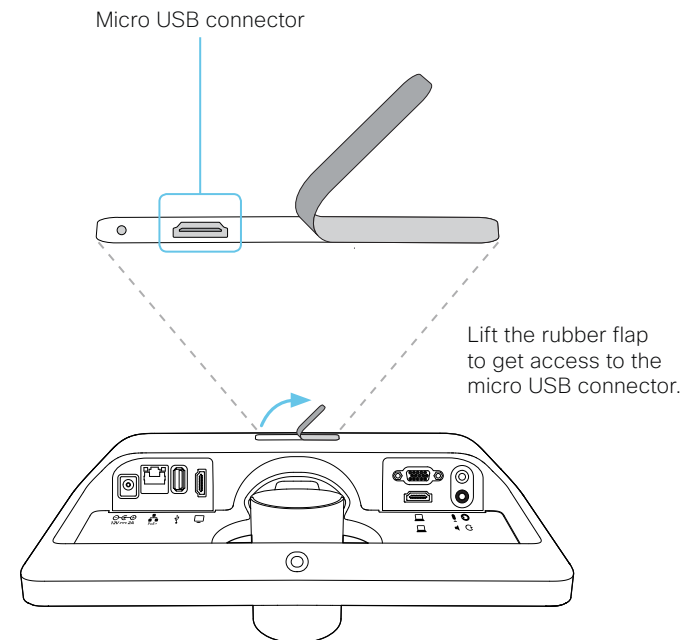
*SerialPort > Mode*

For security reasons, you are asked to sign in before using the serial interface. Use the following setting to change the behavior:

*SerialPort > LoginRequired*

Restart the video system when you have made changes to the serial port settings.

If your video system is provisioned by CUCM, the serial port settings should be configured from CUCM.



## Technical specification (page 1 of 2)

### SOFTWARE COMPATIBILITY

- Cisco TelePresence Software Version TC7.1 or later
- Collaboration Endpoint Software Version 8.0 or later

### PRODUCT DELIVERED WITH:

- SX10 codec with integrated HD camera and microphone
- Wall mount
- TRC6 remote control
- Network and HDMI cables

### INTEGRATED HD CAMERA

- 5x total zoom
- +5°/-25° tilt, ± 30° pan
- 51.5° vertical field of view
- 83° horizontal field of view
- F-value from 2.1
- 1920 × 1080 pixels progressive @ 30fps
- Automatic or manual focus, brightness, and white balance
- Automatic flipping of picture when up-side down

### USER INTERFACE

- TRC6 remote control and on-screen graphical user interface
- Cisco TelePresence Touch 10 (optional)

### LANGUAGE SUPPORT

(depends on software version)

- Arabic, Catalan, Chinese-Simplified, Chinese-Traditional, Czech, Danish, Dutch, English, English-UK, Finnish, French, French-Canadian, German, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese-Brazilian, Russian, Spanish, Spanish-Latin, Swedish, Turkish)

### SYSTEM MANAGEMENT

- Total management using embedded Telnet, SSH, XML, and SOAP
- Remote software upload using web server, SCP, HTTP, and HTTPS
- Remote control and on-screen menu system

### DIRECTORY SERVICES

- Support for local directories (Favorites)
- Corporate directory (through Cisco Unified Communications Manager and Cisco TelePresence Management Suite)
- Server directory supporting LDAP and H.350 (requires Cisco TelePresence Management Suite)
- Call history with received, placed and missed calls with date and time

### POWER

- PoE enabled: 37-57 V, maximum 0.35 A
- Power supply
  - AC input: 1 A, 100-240V, 50-60Hz
  - DC output: 12V, maximum 2 A
- Maximum 12W in normal operation

### OPERATING TEMPERATURE AND HUMIDITY

- Ambient temperature: 0°C to 40°C (32°F to 95°F)
- Relative humidity (RH): 10 to 90%

### STORAGE AND TRANSPORT TEMPERATURE

- -20°C to 60°C (-4°F to 140°F) at RH 10-90% (noncondensing)

### SX10 CODEC DIMENSIONS

- Width: 10.8in. (27.5cm)
- Height: 4.6in. (11.7cm)
- Depth: 3.6in. (9.1cm) (with max camera tilt downward)
- Weight: 2.0lb (0.9kg)

### APPROVALS AND COMPLIANCE

- Directive 2014/35/EU (Low-Voltage Directive)
- Directive 2014/30/EU (EMC Directive) – Class B
- Directive 2011/65/EU (RoHS)
- Directive 2002/96/EC (WEEE)
- NRTL approved (Product Safety)
- FCC CFR 47 Part 15B (EMC) – Class B

Please check Product Approval Status Database [www.ciscofax.com](http://www.ciscofax.com) for approval documents per country.

### BANDWIDTH

- Up to 3Mbps

### MINIMUM BANDWIDTH FOR RESOLUTION AND FRAME RATE

- 720p30 from 768kbps
- 1080p30 from 1472kbps

### FIREWALL TRAVERSAL

- Cisco TelePresence Expressway technology

### VIDEO STANDARDS

- H.263
- H.263+
- H.264

### VIDEO INPUT

Two video inputs (HDMI\* or VGA selectable through user interface). Support formats up to maximum 1280 × 768@30fps, including:

- 640 × 480 (VGA)
- 720 × 480
- 704 × 576 (4CIF)
- 800 × 600 (SVGA)
- 848 × 480
- 1024 × 768 (XGA)
- 1152 × 864 (XGA+)
- 1280 × 720(720p)
- 1280 × 768 (WXGA)

Extended Display Identification Data (EDID)

### VIDEO OUTPUT

One HDMI output\*. Supports format:

- 1920 × 1080 @ 60fps (1080p60)

VESA Monitor Power Management

Extended Display Identification Data (EDID)

\* HDMI version 1.3

## Technical specification (page 2 of 2)

### LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

Supports encode/decode video formats up to maximum 1920 × 1080@30fps (HD1080p30), including:

- 176 × 144 @ 30fps (QCIF) (decode only)
- 352 × 288 @ 30fps (CIF)
- 512 × 288 @ 30fps (w288p)
- 576 × 448 @ 30fps (448p)
- 640 × 480 @ 30fps (VGA)
- 704 × 576 @ 30fps (4CIF)
- 768 × 448 @ 30fps (w448p)
- 800 × 600 @ 30fps (SVGA)
- 1024 × 576 @ 30fps (w576p)
- 1024 × 768 @ 30fps (XGA)
- 1280 × 720 @ 30fps (HD720p)
- 1280 × 768 @ 30fps (WXGA)
- 1920 × 1080 @ 30fps (HD1080p)

### AUDIO STANDARDS

- 64kbps AAC-LD
- OPUS
- G.722
- G.722.1
- G.711mu
- G.711a
- G.729AB
- G.729

### AUDIO FEATURES

- High quality 20kHz audio
- Two acoustic echo cancellers
- Automatic gain control
- Automatic noise reduction
- Active lip synchronization

### AUDIO INPUTS

- One Internal microphone
- One external microphone, 4-pin mini-jack (Cisco TelePresence Table Microphone 20)
- One HDMI audio-in

### AUDIO OUTPUTS

- One line out, mini-jack
- One HDMI (digital main audio)

### DUAL STREAM

- BFCP (SIP) dual stream
- Resolutions up to WXGAp5

### MULTIPOINT SUPPORT

- Cisco ad-hoc conferencing (requires Cisco Unified Communications Manager, Cisco TelePresence Server and Cisco TelePresence Conductor)

### PROTOCOLS

- SIP and H.323

### EMBEDDED ENCRYPTION

- SIP and H.323 point-to-point
- Standards-based: 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)
- Dynamic playout and lip-sync buffering
- Date and time support via NTP
- Packet loss based downspeeding
- URI dialing
- TCP/IP
- DHCP
- IEEE 802.1x network authentication
- IEEE 802.1q Virtual LAN
- IEEE 802.1p QoS and class of service
- Cisco ClearPath

### IPv6 NETWORK SUPPORT

- Dual stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ
- Support for static IP address assignment, stateless autoconfiguration and DHCPv6

### SUPPORTED INFRASTRUCTURE

- Cisco Unified Communications Manager 8.6.2 and later
- Cisco TelePresence Video Communication Server (Cisco VCS)

### SECURITY FEATURES

- Management using web interface (HTTPS/HTTP) and SSH
- Password protected IP administration
- Password protected administration menu
- Disable IP services
- Network settings protection

### NETWORK INTERFACES

- One PoE enabled LAN connector (RJ-45) 10/100Mbps (only auto-negotiation)

### OTHER INTERFACES

- One USB port for future use
- One Micro USB port for maintenance

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](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

December 2016



## 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 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 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

## 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:

*Collaboration Room Endpoints >  
TelePresence SX Series >  
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

### ***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***

- *In-room control guide:* How to design an in-room control panel, and how to use the video system's API to program the in-room controls

### ***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*

## 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

### 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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://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](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (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>.