

Collaboration Endpoint software version 9.10  
DECEMBER 2019



# Administrator guide

for Cisco Webex Codec Plus

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 conferencing device.

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 <https://www.cisco.com/go/room-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>5</b>
User documentation and software .....	6
What's new in CE9.....	7
Codec Plus at a glance.....	34
Power On and Off.....	35
LED indicators .....	37
How to administer the video conferencing device .....	38
<b>Configuration</b> .....	<b>42</b>
User administration .....	43
Change the device passphrase.....	44
Restrict the access to the Settings menu.....	45
Device configuration .....	46
Add a sign in banner .....	47
Add a welcome banner.....	48
Manage the service certificates of the device .....	49
Manage the lists of trusted certificate authorities - CAs.....	50
Set up secure audit logging .....	54
Delete CUCM trust lists.....	55
Change the persistency mode.....	56
Set strong security mode .....	57
Set up ad hoc multipoint conferences.....	58
Set up Intelligent Proximity for content sharing .....	60
Adjust the video quality to call rate ratio.....	65
Add corporate branding to the screen and Touch 10 user interface .....	67
Add a custom wallpaper .....	69
Choose a ringtone and set the ringtone volume .....	70
Manage the Favorites list .....	71
Set up accessibility features.....	72
Provisioning of product specific configurations from CUCM.....	73
<b>Peripherals</b> .....	<b>75</b>
Connect monitors .....	76
Connect input sources.....	78
Extend the number of input sources.....	80
Information about displays.....	81
Information about 4K resolution.....	82
Information about HDMI cables.....	83

Set up the SpeakerTrack feature .....	84	RoomReset settings.....	176
Set up the Snap to Whiteboard feature .....	85	RTP settings.....	177
Set up the PresenterTrack feature .....	88	Security settings .....	178
Classroom set-up .....	92	SerialPort settings.....	181
Connect the Touch 10 controller .....	97	SIP settings.....	182
Connect the ISDN Link.....	101	Standby settings .....	187
<b>Maintenance .....</b>	<b>102</b>	SystemUnit settings.....	189
Upgrade the device software .....	103	Time settings .....	190
Add option keys .....	104	UserInterface settings.....	193
Device status .....	105	UserManagement settings.....	199
Run diagnostics.....	106	Video settings .....	203
Download log files.....	107	WebEngine settings.....	214
Create a remote support user .....	108	Experimental settings .....	215
Backup and restore configurations and custom elements .....	109	<b>Appendices.....</b>	<b>216</b>
CUCM provisioning of custom elements .....	110	How to use Touch 10 .....	217
TMS provisioning of custom elements.....	111	Set up remote monitoring .....	218
Revert to the previously used software image .....	112	Access call information and answer a call while using the web interface.....	219
Factory reset the video conferencing device .....	113	Place a call using the web interface .....	220
Factory reset Cisco Touch 10 .....	116	Share content using the web interface.....	222
Factory reset Cisco TelePresence Touch 10.....	117	Local layout control.....	223
Capture user interface screenshots .....	118	Control a local camera.....	224
<b>Device settings .....</b>	<b>119</b>	Control a far end camera.....	225
Overview of the device settings .....	120	Packet loss resilience - ClearPath.....	226
Audio settings .....	126	Room analytics.....	227
CallHistory settings .....	131	Customize the video conferencing device's Touch 10 user interface.....	229
Cameras settings.....	132	Customize the video conferencing device's behavior using macros .....	231
Conference settings .....	137	Remove default buttons from the user interface .....	232
FacilityService settings.....	142	Use of a third-party USB input device.....	233
H323 settings.....	143	Sending HTTP(S) requests .....	234
HttpClient settings .....	146	Digital signage.....	235
HttpFeedback settings.....	147	API-driven web views .....	236
Logging settings .....	148	Input source composition .....	237
Macros settings .....	150	Presentation source composition .....	239
Network settings.....	151	Manage startup scripts .....	241
NetworkServices settings.....	159	Access the device's XML files .....	242
Peripherals settings .....	166	Execute API commands and configurations from the web interface .....	243
Phonebook settings .....	168	Connector panel .....	244
Provisioning settings.....	170	About Ethernet ports.....	245
Proximity settings.....	173	Mini-jack connector pin-out schemes.....	246
RoomAnalytics settings .....	175	Serial interface for maintenance.....	247

Open TCP Ports.....	248
HTTPFeedback address from TMS.....	249
Link an on-premises registered device to Cisco Webex Edge for Devices .....	250
Register a device to the Cisco Webex cloud service.....	251
Supported RFCs .....	252
Technical specification.....	253
User documentation on the Cisco web site.....	255
Cisco contacts .....	256

## Chapter 1

# Introduction

## User documentation and software

### Products covered in this guide

- Cisco Webex Codec Plus

### User documentation

This guide provides you with the information required to administrate the video conferencing device.

The guide primarily addresses capabilities and configurations of on-premise registered devices (CUCM, VCS), but a sub-set of the capabilities and configurations also applies to devices that are registered to our cloud service (Cisco Webex).

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

### Documentation on the Cisco web site

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

► <https://www.cisco.com/go/room-docs>

### Documentation for cloud registered devices

For more information about devices that are registered to the Cisco Webex cloud service, visit:

► <https://help.webex.com>

### Cisco Project Workplace

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

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

### Software

Download software for the endpoint from the Cisco web site:

► <https://software.cisco.com/download/home>

We recommend reading the Software release notes (CE9):

► <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html>

## What's new in CE9

This chapter provides an overview of the new and changed device settings (configurations), and the new features and improvements in the current Cisco Collaboration Endpoint software version 9.x (CE9.x) compared to CE9.1.

The following Webex products are new in CE9:

- CE9.0 - Room Kit
- CE9.1 - Codec Plus, and Room 55
- CE9.2 - Room 70
- CE9.4 - Codec Pro, Room 70 G2, and Room 55 Dual
- CE9.6 - Room Kit Mini
- CE9.8 - Board 55/55S, Board 70/70S, and Board 85S

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

► <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html>

## New features and improvements in CE9.10

### Webex Edge for Devices

Devices running CE9.10 are ready for *Webex Edge for Devices*. You can use *Webex Edge for Devices* to link your on-premises devices to the Cisco Webex cloud service.

This gives you access to select cloud features, while your registration, device management, calling, and media services remain on-premises. You can manage cloud services and get device diagnostics from them in Webex Control Hub.

You need the Device Connector tool to get started. Read the Release Notes on Webex Help Center to find out when the tool is available.

### Easier to join Webex meetings

We have added a Join Webex button in the user interface. The button is shown by default.

The Join Webex button allows users to join meetings by entering the meeting number without a domain. This information is available in the Webex email invite. The infrastructure must allow calls to be routed to *\*@webex.com*.

### New procedure for defining a password policy

In earlier CE software versions, the password policy was defined using the `systemtools securitysettings` command. This command has now been replaced by configurations (`UserManagement PasswordPolicy *`). Some of the previous restrictions are discontinued.

When upgrading a device from an earlier CE software version, the values previously stored through the `systemtools securitysettings` command are preserved. The ones that are no longer reflected by configurations are deleted. The previous defaults were all 0, so on upgrade, if no changes had been made, the new defaults are also all 0.

### SNMP is switched off by default

SNMP (Simple Network Management Protocol) is switched off by default. Also, we no longer provide a default community name.

When upgrading a device from an earlier CE software version, the values that were previously stored are preserved.

## New features and improvements in CE9.9

### Updates to the UI Extensions editor

(All products)

The *In-room control editor* has been renamed to *UI Extensions editor* to reflect the additional features that are available. You can launch the editor by going to *Integration > UI Extension Editor* on the web interface. In addition, the editor's UI has been updated.

For more information, see the *Customization guide* for CE9.9 at [▶https://www.cisco.com/go/in-room-control-docs](https://www.cisco.com/go/in-room-control-docs)

### Web apps (Boards)

You can use the UI Extensions editor to create web apps. This way you can access apps such as Jira, Miro, Office 365, and Google docs directly from a board.

### Digital signage

(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)

Digital signage allows you to display custom content, such as company news, building maps, or emergency information, when the device is in half-wake mode.

Users can interact with the signage content only on Webex Boards.

### Fetch branding images and custom wallpaper from an external URL (All products)

You can use the `xCommand UserInterface Branding Fetch` API command to download branding images or a custom wallpaper from an external URL.

Custom wallpaper is not available for Webex Boards.

### Changes to the Network Settings menu

(All products)

The Network connection page on the device's user interface has changed. First you see an overview of the current network set-up, then you can open the Ethernet or Wi-Fi settings if you want to change them. A few settings, which were not available from the GUI before, are now added.

### Changes to the ultrasound settings (All products)

All products now has the same default value for the *Audio Ultrasound MaxVolume* setting. Also the volume range is aligned between the different products. Product specific differences are handled internally and no longer reflected in the range of values and the default value. We have not made any changes to the sound level that is played out from a device.

### TLS configuration changes (All products)

For security reasons we have made some changes to the TLS configuration on HTTPS client, syslog, and SIP connections:

- You must explicitly turn off certificate verification if you don't want to perform a certificate check. By default, certificates are checked on all TLS connections.
- The minimum TLS version is increased from version 1.0 to 1.1 (exceptions for CUCM and SIP, which still allow version 1.0). Also note that the Webex cloud is using TLS version 1.2.
- You can configure certificate verification for provisioning, phone book, and other HTTP servers separately. The former *NetworkServices HTTPS VerifyServerCertificate* setting, which covered all these server types, are replaced by three settings: *Provisioning TLSVerify*, *Phonebook Server [1] TlsVerify*, and *HTTPFeedback TlsVerify*.
- You can configure certificate verification for external logging (both audit logging and regular logging).
- For SIP, the certificates are verified against the *Custom CA list*, which is uploaded to the device manually using the web interface or API. For other connections, the certificates are verified against either the *Pre-installed CA list* on the device, or the *Custom CA list*.



## Updates to whiteboarding and annotations

*(Boards)*

- Create, edit, and move stickies on your whiteboard and annotations.
- Choose between three different pen sizes when whiteboarding and annotating.
- Create copies of whiteboards and annotations. The whiteboard or annotated snapshot of a presentation is stored in the Whiteboard menu. You can go back to it and continue work on the copy as you would on any other whiteboard or snapshot.

## Wired touch redirect *(Boards)*

Touch redirect enables you to control your laptop from a Webex Board screen. You must connect the laptop to the Webex Board with an HDMI cable (wired sharing) and a USB-C cable.

Touch redirect only works outside of call.

This feature is only available on the second generation of boards (Webex Board 55S, 70S, and 85S).

## New features and improvements in CE9.8

### New products

The Cisco Webex Boards, which previously have been available only for cloud registration, are now also available for on-premises registration:

- Cisco Webex Board 55/55S
- Cisco Webex Board 70/70S
- Cisco Webex Board 85S

### Support for USB headsets

*(Room Kit, Room Kit Mini, Room 55)*

You can connect a USB Headset, Handset or USB Bluetooth dongle to the USB-A port on the devices. This is similar to the DX series.

### Extended support for HTTP requests *(All products)*

Since CE9.6 a device has been able to send arbitrary HTTP(S) Post and Put requests to an HTTP(S) server. This feature is extended to support more request types (Get, Patch, and Delete), and also to handle data that is returned from the server (response headers and body).

### Improved USB-C experience *(Room Kit Mini)*

The Room Kit Mini is in USB camera mode only when it is streaming media to a computer over the USB-C port. In previous releases it was sufficient that a computer was connected to the USB-C port.

### Add participant to CMS conference from the device UI *(All products)*

Any user can add another participant to an ongoing CMS conference using the user interface of the device. This also includes PSTN calls. When the participant accepts the call, the participant will be added to the same CMS conference.

In this case the device will tell the CMS to dial the participant using the Active Control mechanism. Then the CMS will dial directly to the participant you want to add.

For this feature to work, Active Control must be enabled on the device, the call protocol must be SIP, and the CMS must be on version 2.4 or higher. The feature doesn't work if multipoint mode is set to CUCMMediaResourceGroupList.

### Register a device to Cisco Webex using API or local web interface *(All products)*

You can register a device to Cisco Webex remotely, so you don't have to be in the same room as the device. You can do this programmatically from the API or use the local web interface. In earlier releases you had to use the on-screen setup assistant.

From the web interface, you can only start Webex registering if the device is not currently registered anywhere. If you are using the API, you can start Webex registering even if the device is currently registered to an on-premise system (CUCM or VCS).

### Pre-installed list of Certificate Authorities – CAs *(All products)*

A list of commonly used CA certificates are pre-installed on the video conferencing device. The device uses this list when validating certificates from external servers that it communicates with:

- HTTP servers that host content used by the HttpClient API or macros
- SMTP mail servers (only relevant for Webex Boards)

A factory reset does not delete the list.

### xAPI over WebSocket: Authentication using auth protocol header *(All products)*

Authentication using an auth protocol header is supported. This comes in addition to Basic authentication using an HTTP header field.

This means that browser-based clients, which don't have direct control over HTTP headers, can authenticate to a device directly from the browser using Javascript.

### More device settings can be provisioned from Cisco UCM than before *(All products)*

If the device is registered to Cisco UCM 12.5(1)SU1 more settings and parameters can be provisioned from UCM than before (*Device > Product Specific Configuration Layout*). Also, if these settings are changed locally on the device, the new value can be written back to the UCM.

Most of the device's public settings (xConfiguration), are included. Exceptions are made for Network, Provisioning and SIP settings.

See the *Video Endpoints Management Overview* section in the [► Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5\(1\)SU1](#) for more information.

## New features and improvements in CE9.7

### Connect to xAPI over a WebSocket

*(All products)*

You can now connect to the xAPI over WebSocket. The communication channel over WebSocket is open both ways until it is explicitly closed. This means that the server can send data to the client as soon as the new data is available, and there is no need for re-authentication for every request. This improves speed significantly compared to HTTP.

Each message contains a complete JSON document and nothing else. Many programming languages have good library support for WebSocket and JSON-RPC.

WebSocket is not enabled by default. Note that WebSocket is tied to HTTP and HTTP or HTTPS must be enabled before you can use WebSocket.

For more information, see [▶ xAPI over WebSocket](#) guide.

### Graphical sound mixer available on Audio Console

*(Codec Pro, MX700, MX800, Room 70 G2, Room 70D G2, SX80)*

The Audio Console now has a graphical sound mixer. It has 8 user-definable parametric equalizer settings. A setting consists of up to 6 sections, each of which has its own filter type, gain, center/crossover frequency and Q value. Each section is shown with its own color and the effect of altering any of the parameters immediately becomes visible in the graph.

For more information, see the *Customization guide* for CE9.7 at [▶ https://www.cisco.com/go/in-room-control-docs](https://www.cisco.com/go/in-room-control-docs)

### Ambient noise reporting

*(Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit, Room Kit Mini)*

The Room series devices can be configured to report the stationary ambient noise level in the room. The reported value is an A-weighted decibel value (dBA), which reflects the response of the human ear. Based on reported noise, facility management or a building manager can intervene to troubleshoot the issue.

All signal processing related to this feature is local and the only data transmitted is the calculated noise level.

### Support for multiple SRG-120DH/PTZ-12 cameras *(Codec Plus)*

You can now connect up to three SRG-120DH/PTZ-12 cameras to a Codec Plus using an HDMI and an Ethernet switch.

### Other updates

- 1080p support for Room Kit Mini when it is used as a USB camera. *(Room Kit Mini)*
- You can turn video off and on during calls. *(All products)*
- A system administrator can prevent the use of HTTP and only allow HTTPS Post and HTTPS Put requests. *(All products)*

## New features and improvements in CE9.6

### New product

- Cisco Webex Room Kit Mini

### HDCP support

*(Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)*

One of the device's HDMI inputs can be configured to support HDCP (High-bandwidth Digital Content Protection) protected content. This allows customers to re-purpose the screen by connecting devices such as a Google Chromecast, an Apple TV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the connector is configured to support HDCP, it is reserved for this type of content. This means that you cannot share any content from this specific connector while in a call, not even non-protected content from a laptop.

### Remove default buttons from the user interface

*(All products)*

If you don't need all of the default buttons on the user interface, you can remove the ones that you don't need. This makes it possible to fully customize the user interface. The configuration only removes the buttons, not the functionality as such, and the custom In-Room Control panels can still be exposed.

For more information, see the *Customization guide* at <https://www.cisco.com/go/in-room-control-docs>

### HTTP Post and Put requests *(All products)*

This feature makes it possible to send arbitrary HTTP(S) Post and Put requests from a device to an HTTP(S) server.

By using macros, you can send data to an HTTP(S) server whenever you want. You can choose what data to send, and structure them as you like. This way you can adapt the data to an already established service.

Security measures:

- The HTTP(S) Post/Put feature is disabled by default.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent Post and Put requests is limited.

### Support for 3rd party USB controllers

*(Codec Plus, Codec Pro, DX70, DX80, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit)*

You can use a 3rd party USB input device to control certain functions on a room device. A Bluetooth remote control with a USB dongle and a USB keyboard are examples of such input devices. You can setup the desired features through macros.

This feature is meant to complement the functionality of the Touch 10 or the DX user interfaces. It is not meant to replace the Touch 10 and DX user interfaces.

For more information, see the *Customization guide* at <https://www.cisco.com/go/in-room-control-docs>

### Content priority *(All products)*

You can now configure your device to prioritize bandwidth usage for either Main Video Channel or Presentation Channel.

xConfiguration Video Presentation Priority:  
<Equal, High>

Equal is the default configuration and means 50 / 50 bandwidth division. Selecting "High" divides the bandwidth 25 / 75 in favor of the presentation channel.

### Other updates *(All products)*

- You can start and control recording meetings from the device's user interface, provided that recording is supported by your infrastructure.
- Edit contact's information on UIs.
- SIP calls now display the SIP Session ID field in the logs to help identify calls.
- Ability to use ICE over MRA to locate the best path for media.

## New features and improvements in CE9.5

### Presentation source composition

*(All products except SX10, DX70, DX80)*

With using two or more content sources and sending them as one image, you can create a new experience for sharing in meetings.

This gives users more flexibility with what they present to remote sites. You can configure the presentation composition through in-room controls together with macros or an external controller.

The maximum number of different sources is determined by the device in use:

- *SX20, MX200 G2, MX300 G2, and Room Kit*: two sources
- *Codec Plus, Room 55, Room 55 Dual, and Room 70*: three sources
- *SX80, MX700, MX800, Codec Pro, and Room 70 G2*: four sources

You can only compose content that has been shared through a cable.

### Audio Console on the web interface

*(SX80, Codec Pro)*

The new Audio Console is natively available on the web interface. The audio console gives you simplified tools to route audio from an input to an output. The Audio Console replaces the old java-based CE Console that is no longer maintained.

When you access the Audio Console for the first time you will see the default system audio routes. The Audio Console is controlled by an underlying macro, which is saved and started once you select Choose to overwrite the current device configurations.

For more information, see the *Customization guide* at [▶ https://www.cisco.com/go/in-room-control-docs](https://www.cisco.com/go/in-room-control-docs)

### Classroom set-up

*(SX80, MX700, MX800, Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)*

The Classroom template uses macros to tailor a room set-up that works well for presenting and teaching scenarios. The template provides easy setup, management, and use of the room.

The Classroom set-up works similarly to the Briefing Room set-up (which is available for SX80, Codec Pro, MX700, MX800, and Room 70 G2), but it doesn't require three screens.

### Support for Korean keyboard *(All products)*

Korean keyboard input is supported on Touch 10 when the user interface language is set to Korean.

### Remote monitoring of screen status *(SX20, SX80)*

The remote monitoring of screen status that has been available for the Webex Room series and SX10, is now available for SX20 and SX80.

The codec can wake up the screen from standby mode, or put the screen to standby when the codec enters standby. The input source can also be changed automatically when a call is received.

CEC is disabled on the device by default and must be enabled in the Video Output Connector [n] CEC Mode setting. Your screen must support CEC for remote monitoring to work.

### Welcome banner *(All products)*

You can set up a welcome banner that users see after they sign in to the device's web interface or command line interface. The banner can for example contain information you need in order to get started, or things you must be aware of when setting up the device.

## New features and improvements in CE9.4

### New products

- Cisco Webex Codec Pro
- Cisco Webex Room 55 Dual
- Cisco Webex Room 70 G2

### Rebranding from Cisco Spark to Cisco Webex

*(All products)*

Cisco Spark has changed its name to Cisco Webex, and the user interface elements that displayed *Spark* are changed to *Webex*. In the activation flow you now see Cisco Webex as a registration option instead of Cisco Spark.

The following products have gotten new names:

- Cisco Spark Room Kit is now Cisco Webex Room Kit
- Cisco Spark Room Kit Plus is now Cisco Webex Room Kit Plus
- Cisco Spark Codec Plus is now Cisco Webex Codec Plus
- Cisco Spark Quad Camera is now Cisco Quad Camera
- Cisco Spark Room 55 are now Cisco Webex Room 55
- Cisco Spark Room 70 are now Cisco Webex Room 70
- Cisco DX70 is now Cisco Webex DX70
- Cisco DX80 is now Cisco Webex DX80

### The maximum number of Proximity clients is increased

*(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)*

A Cisco Webex Room Series device can have up to 30 paired clients simultaneously when the Proximity service *ContentShare ToClients* is disabled. If *ContentShare ToClients* is enabled, the limit of paired clients is 7 which is the same as in earlier software versions.

### Support for content sharing using H.263 in a call between Cisco Webex Room Series and legacy MXP devices

*(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)*

Support for H.263 content sharing between MXP and Cisco Webex Room Series is now available. The Room Series previously had a limitation where it could not receive or share content in a separate content channel. Sharing content from a Room Series device to an MXP device would in earlier versions compose the presentation into the main video stream.

This is only supported in certain scenarios:

- Direct H.323 calls (IP dialing) between a Room Series device and an MXP device.
- MXP registered on VCS on H.323 and a Room Series device registered to the same VCS on either SIP or H.323. Note that making an H.323 to SIP call on a VCS requires that an interworking option key is installed on the VCS.

See the CE9 release notes for information on other limitations related to this feature.

### CUCM provisioning of the admin settings lockdown configuration

*(All products)*

The admin settings lockdown configuration, that was introduced in CE9.2.1, can now be provisioned from CUCM. You can lock a selection of the settings on the settings menu on all of your devices simultaneously when you configure them through CUCM.

Your CUCM may require a new device package in order to expose the new fields for this configuration.

### Enable backlight compensation from the user interface

*(DX70, DX80)*

A new setting on the DX70 and DX80 main menu enables and disables backlight compensation. This is a fixed setting that increases (on) or decreases (off) the sensors brightness levels in order to compensate for sunlight or other bright light sources behind the user. The backlight compensation sets the sensor to a fixed level and it is not auto adjusted to the backlight.

### Changed default HTTP mode from HTTP+HTTPS to HTTPS

*(All products)*

The default value of *NetworkServices HTTP Mode* is changed from HTTP+HTTPS to HTTPS. This is to increase the security of the room devices on default configuration. Upgrading from earlier software versions will not automatically change the default value and it will stay on HTTP+HTTPS to avoid breaking current HTTP implementations.

The change is seen on new devices running CE9.4.0 or later, or if the device is factory reset on CE9.4.0. The HTTP requests are redirect to HTTPS and on the first visit to the device's web interface, the device displays an "Insecure connection warning". To proceed to the web interface, you need to create an exception in your browser. This is a one-time operation unless you access the web interface with a different browser that has never visited the device web interface or if the device is factory reset.

### In-Room Control update

*(All products)*

You can add buttons for as many panels as you want on the home screen as well as on the in-call screen of the user interface.

## New features and improvements in CE9.3

### Backup and restore settings and custom elements (All products)

You can include custom elements as well as configurations in a backup file bundle (zip). You can choose which of the following elements to include in the bundle:

- Branding images
- Macros
- Favorites
- Sign-in banner
- In-room control panels
- Configurations (all or a sub-set)

In previous software versions, you could only backup the configurations.

The backup file can either be restored manually from the device's web interface, or you can generalize the backup bundle so that it can be provisioned across multiple devices, for example using Cisco UCM or TMS.

You will find the backup and restore functionality under *Maintenance > Backup and Restore* on the device's web interface.

### Provisioning of custom elements (All products)

The backup bundle, as described above, can be provisioned to many devices using Cisco UCM or TMS. It is important that device specific information is removed when creating a backup bundle intended for multiple devices. If you include device specific information in such a bundle, you may end up with multiple devices that cannot be reached.

By provisioning a non-device specific backup bundle, you can for example, copy a device's setup with macros, branding elements, and in-room control panels across multiple devices.

Currently, provisioning via Cisco UCM will not restore any configurations, only the other custom elements; TMS will restore everything that is included in the backup bundle.

See the release note for more details about provisioning.

### In-Room Control updates (All products)

The following functionality is added to the in-room control feature:

- You can add buttons for up to 20 panels in total. The buttons appear on the home screen or the in-call screen of the user interface depending on the panel type.
- As before, there are three types of in-room control panels: global panels (always available), in-call panels (available only when in call), and out-of-call panels (only available when not in a call). The entry point for the global panel has been removed from the status bar (top right corner of the user interface). Buttons to open global panels are added to both the home screen and the in-call screen instead, together with the buttons for the out-of-call only and in-call only panels, respectively.
- You can make standalone trigger-buttons, which are buttons that trigger an event directly, without opening a panel on the user interface.

Also the following features are added in the in-room control editor:

- Some new icons are available.
- A set of colors to choose from for the in-room-control buttons.
- Double click text elements to edit text directly.
- Drag and drop in-room control XML files into the editor.

For a full description of in-room controls, see the *Customization guide* at ► <https://www.cisco.com/go/in-room-control-docs>

### Support for ISDN Link (All products)

ISDN Link with software version IL1.1.7 is supported for all devices that supports CE9.3.0.

As before, when using automatic pairing (which allows the ISDN Link to be automatically discovered by the video conferencing device) IPv6 must be enabled on the video conferencing device.

### One Button to Push snooze (All products)

You are able to snooze an One Button to Push (OBTP) meeting reminder for 5 minutes. The snooze time cannot be changed. The reminder typically appears if you are in a call and a scheduled meeting is about to start. You can snooze the reminder for 5 minutes each time it appears until the meeting has ended.

### Adjust the call rate before making a call

(All products)

As soon as you start typing in the *Search or dial* field, you can open a dialog and select a custom call rate. In earlier releases this was available only when selecting an entry from the Directory.

If you don't select a custom call rate, you get the rate set in the *Conference DefaultCall Rate* setting.

### Select ring-tone and adjust ring-tone volume

(All products)

You can select a ring-tone and adjust the ring-tone volume from the settings menu on the user interface. In the previous releases this was done from the web interface.

### Resume a postponed upgrade (All products)

When you get a notification about software upgrade, you can choose *Upgrade now* or *Postpone*. If you postpone the upgrade, you can resume the upgrade from the *Settings > About this device* menu on the user interface when you are ready; you don't have to wait for 6 hours like you had to before.

If you don't manually resume the upgrade, the upgrade will start automatically after 6 hours.

### Prevent device information from being exposed in the user interface (All products)

You can prevent important device information from being exposed in the user interface, for example:

- IP addresses (video conferencing device, touch controller, UCM/VCS registrar)
- MAC address
- Serial number
- Software version

To enable this feature the following must be done:

- A passphrase must be set for all users with administrator rights
- *UserInterface SettingsMenu Mode* must be set to Locked
- *UserInterface Security Mode* must be set to Strong

This feature also means that the IP address is not displayed on the screen when you disconnect a Touch controller.

### Mirrored self-view (DX70, DX80)

You can configure the device to show the self-view image the way other people see you, or as you would see yourself in a mirror. Use the *Video Selfview Mirrored* setting. Mirrored self-view used to be available only for Cisco DX devices running Android software.

Mirroring only applies to the self-view image, and has no effect on the video that is sent to the far end.

### Accessibility: Flashing screen on incoming calls

(All products)

You can configure the device so that the screen and Touch controller flashes red / light grey when the device receives an incoming call. This feature is mainly targeting hearing impaired users, making it easier for them to notice an incoming call.

The feature is disabled by default, and must be enabled by the *Accessibility IncomingCallNotification* setting.

### Screen status monitoring and control (SX10)

SX10 now has the same CEC (Consumer Electronics Control) behavior as the devices in the Room series.

The device will use CEC to set the screen in standby when the device itself enters standby, and wake up the screen and select the correct video input when the device itself wakes up from standby. CEC information from the screen is included in the device's status. Of course, the screen must also support CEC and send the relevant information to the device.

CEC is disabled on the device by default, and must be enabled in the *Video Output Connector [1] CEC Mode* setting.

### One common API guide (All products)

We have gathered all API information in **one** API guide, that covers all products. This is in contrast to earlier releases where we have had one API guide per product.



## New features and improvements in CE9.2

### New product

- Cisco Webex Room 70 (formerly Cisco Spark Room 70)

### Macro framework *(All products except SX10)*

The macro framework allows users and integrators to write JavaScript macros in order to automate scenarios and customize endpoint behavior so that it suits an individual customer's requirements.

The combination of macros and powerful features such as listening for events/status changes, automating execution of commands and configurations, and providing local control functionality for the In-Room control feature, provides many possibilities for custom setups.

Minor behavioral changes, such as having the device in Do Not Disturb for an infinite amount of time, can be easily realized by macros. Some other examples are: Reset configurations automatically, make a call at a certain time of the day, and issue alert or help messages depending on status changes.

The macro editor, which also provides several example macros, is available from the device's web interface.

### HDCP support *(Room 55)*

The device's second HDMI input (Connector 3) can be configured to support HDCP (High-bandwidth Digital Content Protection) protected content. This allows customers to re-purpose the device's screen by connecting devices such as a Google ChromeCast, an AppleTV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the connector is configured to support HDCP, it is reserved for this type of content. This means that you cannot share any content from this specific connector while in a call, not even non-protected content from a laptop.

### Branding and halfwake customization

*(All products except SX10)*

You can upload your own text and images to customize the appearance of the screen and user interface in both the halfwake state and the awake state.

In the *Halfwake* state you can:

- Add a background brand image to the screen and user interface.
- Add a small logo in the bottom right corner of the screen and user interface.

In the *Awake* state you can:

- Add a small logo in the bottom right corner of the screen and user interface.
- Add a label or message in the bottom left corner of the screen (not the user interface).

### Source composition *(All products except SX10, DX70, DX80)*

You can compose up to four input sources (depending on how many input sources are available on the codec) into one image. This is the image that will be sent in the main video stream to the far end in a call. Source composition can only be enabled via the API, so we recommend creating a user interface extension combined with a macro to control the compositions on demand.

This feature replaces some of the functionality that was provided by the TC Console application for TC software.

### HTTP Proxy support *(All products)*

You can set up the device to go through a HTTP Proxy when registering it to Cisco's cloud service, Cisco Spark.

### User interface features *(All products)*

- The Settings panel is restructured.
- The Settings panel in the user interface can be protected by the device's admin password. If the password is blank, anyone can access the Settings and factory reset the device.
- If you select the Russian language on the user interface, you can choose between a Russian keyboard and a keyboard with a Latin character set.
- Arabic and Hebrew languages are added to the user interface. Also localized keyboards are included.
- Basic IEEE 802.1x settings are added to the Settings panel in the user interface.

### Cisco TelePresence Precision 60 Camera support *(Codec Plus, Room 70)*

You can connect Cisco TelePresence Precision 60 cameras to Codec Plus. Note that you need a switch for the camera control cables if you have more than one camera. The People Count feature is not supported if Precision 60 is the only camera type connected to the codec.

### Cisco Spark Quad Camera support *(SX80)*

You can connect a Cisco Spark Quad Camera to the SX80. Note that the Quad Camera uses only one of the codec's HDMI inputs, while the SpeakerTrack 60 camera uses two. The People Count feature (in call) is also available when using the Quad Camera.

## Support for the Snap to Whiteboard feature

*(SX80, MX700, MX800, Codec Plus, Room Kit, Room 55, Room 70)*

The Snap to Whiteboard feature is now available for all products that have a camera with speaker track functionality: SX80 with Cisco TelePresence Speaker Track 60 camera or Cisco Spark Quad Camera, MX700/MX800 with dual camera, Room Kit, Room Kit Plus, Room 55 and Room 70.

When the device detects a person that is speaking close to the whiteboard, the camera view will switch to the whiteboard area. The wizard in the Settings panel on the Touch 10 user interface helps you to set up the feature and define where the whiteboard area is.

## Briefing Room mode *(SX80, MX700, MX800)*

The Briefing Room feature, which was introduced already in TC software, has been reworked. The in-room control framework is used for creating the associated user interface elements.

For MX700 and MX800, Briefing Room is supported only for dual camera devices. Also, you need a Precision 60 camera, and a total of three screens.

For SX80, Briefing Room is supported when a speaker track camera, a Precision 60 camera, and three screens are connected. The speaker track camera can be either Cisco TelePresence SpeakerTrack 60 or Cisco Spark Quad Camera.

## USB to Serial port support

*(Codec Plus, Room Kit, Room 55, Room 70)*

You can connect a USB (Type A) to serial (D-sub 9) adapter to access the device's API. Cisco recommends the UC232R-10 USB to RS232 (FTDI) adapter.

## Mute and unmute remote participants in a CMS hosted conference – Active Control *(All products)*

When a device is enabled for Active Control in a CMS (2.1 or later) conference you can mute and unmute remote participants from the participant list on the user interface (the feature must also be enabled on the CMS).

A device that is running software version CE9.2 will not be unmuted directly. When you try to unmute such a device remotely, a message will show up on its screen requesting the user to unmute the audio locally.

## API commands for Custom input prompt

*(All products)*

API commands are introduced to allow for an input prompt in the user interface: `xCommand UserInterface Message TextInput *`. When issuing the display command a prompt with your custom text, a text input field for the user, and a submit button, shows up on the user interface. For example, you can prompt a user to leave feedback after an ended call. You can specify what type of input you want from the user: single line text, numeric, password, or PIN code.

The prompt can only be enabled via the API, so it is recommended to combine it with macros and either a custom user interface panel or an auto-triggered event.

## Certificate upload via API *(All products)*

ASCII PEM formatted certificates can be installed directly using multiline API commands (`xCommand Security Certificates CA Add`, or `xCommand Security Certificates Services Add`). You can also upload certificates to a device from its web interface, as before.

## API commands for user management *(All products)*

You can create and manage user accounts directly using API commands (`xCommand UserManagement User *`). As before, you can also do this from the device's user interface.

## Preview mode for In-Room Controls *(All products)*

The In-Room Control editor has a new preview mode. A virtual touch interface shows how the design looks. The user interface is interactive so that you can test the functionality. It produces real events on the device, which can trigger any functionality you have created with a third-party control system. A console in the right pane displays both the widget values when interacted with, and control system feedback messages.

## Intelligent Proximity changes *(All products)*

A Proximity indicator is displayed on the screen (middle right) to inform that one or more clients are paired to the device with Cisco Proximity. The old indicator (top left), which was always shown when Proximity was enabled, has been removed.

You can no longer disable the Proximity services from the user interface.

The ultrasound settings have moved from Peripherals Pairing Ultrasound to Audio Ultrasound.

### Automatic factory reset when changing the call service – device activation *(All products)*

The device will automatically factory reset and restart when using the user interface to change the device activation method, for example from VCS to Cisco UCM. This will prevent conflicting configurations when provisioning the device to a new service.

Changing the provisioning from the API will not automatically factory reset the device.

### Support for separate RTP port ranges for audio and other media *(All products)*

You can configure the device so that audio uses a different RTP port range than other media. The two ranges cannot overlap. As default, all media use the same RTP port range.

## Configuration changes in CE9.10

### New configurations

Cameras SpeakerTrack Closeup *(Boards)*

Macros UnresponsiveTimeout *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2, DX80, DX70)*

Macros XAPI Transport *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2, DX80, DX70)*

Peripherals Pairing CiscoTouchPanels RemotePairing *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

Provisioning WebexEdge *(All products)*

Proximity AlternatePort Enabled *(All products)*

Security Fips Mode *(All products)*

UserInterface Assistant Mode *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

UserInterface Assistant ProactiveMeetingJoin *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

UserInterface Features Call JoinWebex *(All products)*

UserManagement PasswordPolicy Complexity MinimumDigits *(All products)*

UserManagement PasswordPolicy Complexity MinimumLength *(All products)*

UserManagement PasswordPolicy Complexity MinimumLowercase *(All products)*

UserManagement PasswordPolicy Complexity MinimumSpecial *(All products)*

UserManagement PasswordPolicy Complexity MinimumUppercase *(All products)*

UserManagement PasswordPolicy MaxLifetime *(All products)*

UserManagement PasswordPolicy ReuseLimit *(All products)*

Video Input Connector [n] OptimalDefinition Threshold60fps *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

### Configurations that are removed

None.

### Configurations that are modified

Cameras SpeakerTrack Closeup *(Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, MX700, MX800)*

**OLD:** Auto/Off

**NEW:** Auto/Off/On

NetworkServices SMTP Security *(Boards)*

**OLD:** Default: None

**NEW:** Default: StartTIs

NetworkServices SNMP Mode *(All products)*

**OLD:** Default: ReadOnly

**NEW:** Default: Off

Standby Signage Mode *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

Video Input Connector [n] OptimalDefinition Threshold60fps *(SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)*

**OLD:** Default: 1280\_720

**NEW:** Default: 1920\_1080

## Configuration changes in CE9.9

### New configurations

Audio Input ARC [1] Mode *(Codec Plus)*

Audio Input HDMI [2..3] Level *(Room 55D, Room 70)*

Audio Input HDMI [2..3] Mode *(Room 55D, Room 70)*

Audio Input HDMI [2..3] VideoAssociation MuteOnInactiveVideo *(Room 55D, Room 70)*

BYOD TouchForwarding Enabled *(Boards)*

*Not available in CE9.9.0.*

HttpFeedback TlsVerify *(All products)*

Logging External TlsVerify *(All products)*

Phonebook Server [1] TlsVerify *(All products)*

Provisioning TlsVerify *(All products)*

Standby Signage Audio *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

Standby Signage InteractionMode *(Boards)*

Standby Signage Mode *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

Standby Signage RefreshInterval *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

Standby Signage Url *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

UserInterface WebcamOnlyMode *(Room Kit Mini)*

WebEngine Mode *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

WebEngine RemoteDebugging *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards)*

### Configurations that are removed

NetworkServices HTTPS VerifyServerCertificate *(All products)*

Replaced by:

- HttpFeedback TlsVerify
- Phonebook Server [1] TlsVerify
- Provisioning TlsVerify

### Configurations that are modified

Audio Ultrasound MaxVolume *(All products)*

*The valuespace and default value has changed for many products. Product specific differences are now handled internally and not reflected in the default value and range of possible values.*

**NEW valuespace:** Integer (0..90) *(Codec Pro, Codec Plus, SX80, SX20)*

**NEW valuespace:** Integer (0..70) *(Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, Boards, SX10, MX700, MX800, MX200 G2, MX300 G2, DX70, DX80)*

**NEW default value:** 70 *(All products)*

RTP Ports Range Stop *(All products)*

**OLD:** Default: 2486

**NEW:** Default: 2487

**OLD:** Integer (1120..65535)

**NEW:** Integer (1121..65535)

SIP ListenPort *(All products)*

**OLD:** Off/On

**NEW:** Auto/Off/On

SIP ListenPort *(Boards)*

**OLD:** Default: On

**NEW:** Default: Auto

SIP TlsVerify *(All products)*

**OLD:** Default: Off

**NEW:** Default: On

Video Output Connector [n] Location HorizontalOffset *(Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)*

OLD: Integer (-100..100)

NEW: String (1, 12)

Video Output Connector [n] Location VerticalOffset *(Codec Pro, Codec Plus, Room Kit, Room 55, Room 55D, Room 70, Room 70 G2, SX80, SX20, MX700, MX800, MX200 G2, MX300 G2)*

OLD: Integer (-100..100)

NEW: String (1, 12)

## Configuration changes in CE9.8

### New configurations

Conference Multipoint Mode *(SX10, DX70, DX80)*

NetworkServices SMTP From *(Boards)*

NetworkServices SMTP Mode *(Boards)*

NetworkServices SMTP Password *(Boards)*

NetworkServices SMTP Port *(Boards)*

NetworkServices SMTP Security *(Boards)*

NetworkServices SMTP Server *(Boards)*

NetworkServices SMTP Username *(Boards)*

SerialPort LoginRequired *(Codec Pro, Room 70 G2)*

UserInterface Phonebook DefaultSearchFilter *(All products)*

UserInterface SoundEffects Mode *(All products)*

### Configurations that are removed

Video DefaultLayoutFamily Remote *(SX10, DX70, DX80)*

### Configurations that are modified

Audio KeyClickDetector Attenuate *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

**OLD:** Default: On

**NEW:** Default: True

**OLD:** Off/On

**NEW:** False/True

Audio KeyClickDetector Enabled *(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

**OLD:** Default: Off

**NEW:** Default: True

**OLD:** Off/On

**NEW:** False/True

Audio Output Line[1..6] Delay Mode *(Room 70 G2)*

**OLD:** Default: RelativeToHDMI

**NEW:** Default: Fixed

## Configuration changes in CE9.7

### New configurations

HttpClient AllowHTTP *(All products)*

Logging Debug Wifi *(Codec Plus, Codec Pro, DX70, DX80, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

Logging Internal Mode *(All products)*

NetworkServices Websocket *(All products)*

Phonebook Server [1] Pagination *(All products)*

RoomAnalytics AmbientNoiseEstimation Mode *(Codec Plus, Codec Pro, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

UserInterface Features Call VideoMute *(Codec Plus, Codec Pro, MX200 G2, MX300 G2, MX700, MX800, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, SX10, SX20, SX80)*

UserInterface Features Whiteboard Start *(DX70, DX80)*

UserInterface Phonebook Mode *(All products)*

UserInterface SettingsMenu Visibility *(All products)*

UserInterface UsbPromotion *(Room Kit Mini)*

### Configurations that are removed

RoomAnalytics PeopleCountOutOfCall *(MX700, MX800)*

### Configurations that are modified

Audio Input Line [1..4] VideoAssociation VideoInputSource *(MX700, MX800, SX80)*

OLD: 1/2/3/4/5

NEW: 1/2/3/4

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(Codec Pro, Room 70 G2)*

OLD: 1/2/3/4/5

NEW: 1/2/3/4/5/6

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(MX700, MX800, SX80)*

OLD: 1/2/3/4/5

NEW: 1/2/3/4

Video Input Connector [6] CameraControl Mode *(Codec Pro, Room 70 G2)*

OLD: Default: On

NEW: Default: Off

OLD: On

NEW: On/Off

Video Presentation Priority *(All products)*

OLD: Equal/High

NEW: Equal/High/Low



## Configuration changes in CE9.6

### New configurations

Audio Input Microphone [1..8] Channel *(Codec Pro, Room 70 G2)*

Audio Input HDMI [n] Level *(Codec Plus, Room 55, Room 70 G2, Room Kit)*

Audio Input HDMI [n] Mode *(Room 70 G2, Room Kit)*

Audio Input HDMI [2..5] VideoAssociation MuteOnInactiveVideo *(Room 70 G2)*

Audio Microphones PhantomPower *(Codec Plus, MX200 G2, MX300 G2, Room 55, Room Kit, SX20)*

Audio Output ConnectorSetup *(Codec Pro, Room 70 G2)*

Audio Output HDMI [n] Level *(MX700, MX800)*

Audio Output HDMI [n] Mode *(Codec Plus, MX700, MX800)*

Audio Output InternalSpeaker Mode *(MX700, MX800, Room 55 Dual, Room 70)*

Audio Output Line [1..6] Equalizer ID *(Room 70 G2)*

Audio Output Line [1..6] Equalizer Mode *(Room 70 G2)*

HttpClient AllowInsecureHTTPS *(All products)*

HttpClient Mode *(All products)*

NetworkServices NTP Server [1..3] Key *(All products)*

NetworkServices NTP Server [1..3] KeyId *(All products)*

NetworkServices NTP Server [1..3] KeyAlgorithm *(All products)*

Peripherals InputDevice Mode *(DX70, DX80)*

UserInterface Branding AwakeBranding Colors *(All products)*

UserInterface Features Call End *(All products)*

UserInterface Features Call MidCallControls *(All products)*

UserInterface Features Call Start *(All products)*

UserInterface Features HideAll *(All products)*

UserInterface Features Share Start *(All products)*

Video Input Connector [n] HDCP Mode *(Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)*

Video Output Connector [2] CEC Mode *(Room 70 Single)*

Video Presentation Priority *(All products)*

### Configurations that are removed

Conference MultiStream Mode *(MX200 G2, MX300 G2, SX20)*

SIP PreferredIPMedia *(All products)*

### Configurations that are modified

Audio Output ARC [1] Mode *(Codec Pro, Room 70 G2)*

**OLD:** Default: Auto

**NEW:** Default: On

**OLD:** Value space: Off / On / Auto

**NEW:** Value space: Off / On

Audio Output HDMI [1..3] Mode *(Codec Pro, Room 70 G2)*

**OLD:** Default: Auto *(Codec Pro)*

**NEW:** Default: On *(Codec Pro)*

**OLD:** Default, HDMI [2..3]: Auto *(Room 70G2 Single)*

**NEW:** Default, HDMI [2..3]: Off *(Room 70G2 Single)*

**OLD:** Default, HDMI [3]: Auto *(Room 70G2 Dual)*

**NEW:** Default, HDMI [3]: Off *(Room 70G2 Dual)*

**OLD:** Value space: Off / On / Auto *(Codec Pro, Room 70 G2)*

**NEW:** Value space: Off / On *(Codec Pro, Room 70 G2)*

Audio Output InternalSpeaker Mode *(Room 55, Room 70 G2, Room Kit)*

**OLD:** Default: Auto *(Room 70 G2)*

**NEW:** Default: On *(Room 70 G2)*

**OLD:** Value space: Off / On / Auto *(Room 70 G2)*

**NEW:** Value space: Off / On / UltrasoundOnly *(Room 70 G2)*

**OLD:** Value space: Off / On *(Room 55, Room Kit)*

**NEW:** Value space: Off / On / UltrasoundOnly *(Room 55, Room Kit)*

Audio Ultrasound MaxVolume *(SX20)*

**OLD:** Default: 70

**NEW:** Default: 60

Provisioning Mode *(All products)*

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

**NEW:** Value space: Auto / CUCM / Edge / Off / TMS / VCS / Webex

Provisioning Mode *(Room 55 Dual)*

**OLD:** Default: Off

**NEW:** Default: On

Standby WakeupOnMotionDetection *(Room 55 Dual)*

**OLD:** Default: Off

**NEW:** Default: On

## Configuration changes in CE9.5

### New configurations

Audio Input ARC [n] Mode *(Codec Pro, Room 70 G2)*  
Audio Output ARC [1] Delay DelayMs *(Codec Pro, Room 70 G2)*  
Audio Output ARC [1] Delay Mode *(Codec Pro, Room 70 G2)*  
Audio Output ARC [1] Mode *(Codec Pro, Room 70 G2)*  
Audio Output InternalSpeaker Mode *(Room 70 G2)*  
Audio Output Line [1] Mode *(Codec Plus, Room 55)*  
Audio Output Line [1] OutputType *(Codec Plus, Room 55)*  
NetworkServices SSH HostKeyAlgorithm *(All products)*  
Peripherals InputDevice Mode *(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)*  
RoomAnalytics PeopleCountOutOfCall *(SX80)*

### Configurations that are removed

Audio Output InternalSpeaker Mode *(Codec Pro)*  
Cameras SpeakerTrack ConnectorDetection CameraLeft *(Room 70 G2)*  
Cameras SpeakerTrack ConnectorDetection CameraRight *(Room 70 G2)*  
Cameras SpeakerTrack ConnectorDetection Mode *(Room 70 G2)*  
Cameras SpeakerTrack TrackingMode *(Room 70 G2)*  
Provisioning RoomType ClassroomEnabled *(SX80, MX700, MX800, Codec Pro, Room 70 G2)*

### Configurations that are modified

Audio Input Microphone[1..8] Equalizer ID *(Codec Pro, Room 70 G2)*  
**OLD:** Value space: Integer (1..14)  
**NEW:** Value space: Integer (1..8)  
Audio Ultrasound MaxVolume *(SX80, MX700, MX800, Codec Pro, Room 70 G2)*  
**OLD:** Default value: 70 *(SX80, Codec Pro, MX700, MX800, Room 70 G2)*  
**NEW:** Default value: 60 *(SX80, Codec Pro, Room 70 G2)*  
**NEW:** Default value: 66 *(MX700, MX800)*  
**OLD:** Value space: Integer (0..90) *(Room 70 G2)*  
**NEW:** Value space: Integer (0..80) *(Room 70 G2)*  
Cameras PresenterTrack Connector *(Codec Plus, Codec Pro, Room 70, Room 70 G2)*  
**OLD:** Default value: 1 *(Codec Pro, Room 70 G2)*  
**NEW:** Default value: 6 *(Codec Pro, Room 70 G2)*  
**OLD:** Value space: Integer (1..5) *(Codec Plus, Codec Pro, Room 70, Room 70 G2)*  
**NEW:** Value space: Integer (1..3) *(Codec Plus, Room 70)*  
**NEW:** Value space: Integer (1..6) *(Codec Pro, Room 70 G2)*  
Video Input Connector [3,4,5] PreferredResolution *(Codec Pro, Room 70 G2)*  
**OLD:** Default value: 3840\_2160\_30  
**NEW:** Default value: 1920\_1080\_60

## Configuration changes in CE9.4

### New configurations

Audio Input HDMI [1..2] Mode *(Room 55)*

Audio Input HDMI [1..2] VideoAssociation MuteOnInactiveVideo *(Room 55)*

Audio Output Line [1] OutputType *(Room 70)*

Cameras Camera [1] Backlight DefaultMode *(DX70, DX80)*

Cameras Camera [1..2] Mirror *(MX700, MX800)*

Conference FarendMessage Mode *(All products)*

SIP MinimumTLSVersion *(All products)*

### Configurations that are removed

NetworkServices HTTP Proxy Allowed *(All products)*

Video Output Connector [2] CEC Mode *(DX70, DX80)*

Video Output Connector [2] Location HorizontalOffset *(DX70, DX80)*

Video Output Connector [2] Location VerticalOffset *(DX70, DX80)*

Video Output Connector [2] OverscanLevel *(DX70, DX80)*

Video Output Connector [2] Resolution *(DX70, DX80)*

Video Output Connector [2] RGBQuantizationRange *(DX70, DX80)*

### Configurations that are modified

Audio Output Line [1] OutputType *(Room Kit)*

**OLD:** Default value: LineOut

**NEW:** Default value: Loudspeaker

**OLD:** Value space: LineOut / Subwoofer

**NEW:** Value space: LineOut / Loudspeaker / Recorder / Subwoofer

Audio Ultrasound MaxVolume *(MX200 G2, MX300 G2, Codec Plus, Room 55, Room 70)*

**OLD:** Default value: 60 *(MX200 G2, MX300 G2)*

**OLD:** Default value: 70 *(Codec Plus, Room 55, Room 70)*

**NEW:** Default value: 50 *(MX200 G2, MX300 G2)*

**NEW:** Default value: 60 *(Codec Plus, Room 70)*

**NEW:** Default value: 64 *(Room 55)*

**OLD:** Value space: Integer (0..80) *(MX200 G2, MX300 G2)*

**OLD:** Value space: Integer (0..90) *(Room 55, Room 70)*

**NEW:** Value space: Integer (0..70) *(MX200 G2, MX300 G2)*

**NEW:** Value space: Integer (0..80) *(Room 70)*

**NEW:** Value space: Integer (0..84) *(Room 55)*

Network [1] DNS DNSSEC Mode *(All products)*

**OLD:** User role: ADMIN, USER

**NEW:** User role: ADMIN

Network [1] Speed *(All products)*

**OLD:** User role: ADMIN, USER

**NEW:** User role: ADMIN, INTEGRATOR

NetworkServices HTTP Mode *(All products)*

**OLD:** Default value: HTTP+HTTPS

**NEW:** Default value: HTTPS

NetworkServices SNMP CommunityName *(All products)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

NetworkServices SNMP Host [1..3] Address *(All products)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

NetworkServices SNMP Mode *(All products)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

NetworkServices SNMP SystemContact *(All products)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

NetworkServices SNMP SystemLocation *(All products)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

UserInterface ContactInfo Type *(SX10, DX70, DX80)*

**OLD:** Value space: Auto / DisplayName / IPv4 / IPv6 / None / SipUri / SystemName

**NEW:** Value space: Auto / DisplayName / E164Alias / H320Number / H323Id / IPv4 / IPv6 / None / SipUri / SystemName

Video Output Connector [1] CEC Mode *(SX10)*

**OLD:** Default value: Off

**NEW:** Default value: On

Video Output Connector [3] Resolution *(SX80)*

**OLD:** User role: ADMIN, INTEGRATOR

**NEW:** User role: ADMIN, INTEGRATOR, USER

## Configuration changes in CE9.3

### New configurations

Audio KeyClickDetector Attenuate *(Codec Plus, Room Kit, Room 55, Room 70)*

Audio KeyClickDetector Enabled *(Codec Plus, Room Kit, Room 55, Room 70)*

Cameras Camera [1..3] AssignedSerialNumber *(Codec Plus, Room 70)*

Cameras Camera [3] Backlight DefaultMode *(Codec Plus, Room 70)*

Cameras Camera [3] Brightness DefaultLevel *(Codec Plus, Room 70)*

Cameras Camera [3] Brightness Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Focus Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Gamma Level *(Codec Plus, Room 70)*

Cameras Camera [3] Gamma Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Mirror *(Codec Plus, Room 70)*

Cameras Camera [3] Whitebalance Level *(Codec Plus, Room 70)*

Cameras Camera [3] Whitebalance Mode *(Codec Plus, Room 70)*

Network [1] DNS DNSSEC Mode *(All products)*

NetworkServices HTTP Proxy PACUrl *(All products)*

SystemUnit CrashReporting Advanced *(All products)*

SystemUnit CrashReporting Mode *(All products)*

SystemUnit CrashReporting URL *(All products)*

UserInterface Accessibility IncomingCallNotification *(All products)*

UserInterface Security Mode *(All products)*

Video Selfview Mirrored *(DX70, DX80)*

### Configurations that are removed

Provisioning HttpMethod *(All products)*

### Configurations that are modified

NetworkServices HTTP Proxy Allowed *(All products)*

**OLD:** Default value: True

**NEW:** Default value: False

NetworkServices HTTP Proxy Mode *(All products)*

**OLD:** Value space: Manual/Off

**NEW:** Value space: Manual/Off/PACUrl/WPAD

Proximity Mode *(Room 70)*

**OLD:** Default value: Off

**NEW:** Default value: On

Security Session MaxSessionsPerUser *(All products)*

**OLD:** Default value: 0

**NEW:** Default value: 20

**OLD:** Value space: Integer (0..100)

**NEW:** Value space: Integer (1..20)

Security Session MaxTotalSessions *(All products)*

**OLD:** Default value: 0

**NEW:** Default value: 20

**OLD:** Value space: Integer (0..100)

**NEW:** Value space: Integer (1..20)

Standby WakeupOnMotionDetection *(Room 70)*

**OLD:** Default value: Off

**NEW:** Default value: On

Video Input Connector[2] Name *(Room 55)*

**OLD:** Default value: "PC 1 (HDMI)"

**NEW:** Default value: ""

Video Input Connector[3] Name *(Room 55)*

OLD: Default value: "PC 2 (HDMI)"

NEW: Default value: ""

Video Input Connector[1] CEC Mode *(Room 70)*

OLD: Value space: Off/On

NEW: Value space: On

## Configuration changes in CE9.2

### New configurations

Audio Input HDMI[n] Mode *(Codec Plus)*

Audio Input HDMI[n] VideoAssociation MuteOnInactiveVideo *(Codec Plus, Room Kit)*

Audio Output InternalSpeaker Mode *(Room 55)*

Audio Ultrasound MaxVolume *(All products)*

*Replacing Peripherals Pairing Ultrasound Volume MaxLevel*

Audio Ultrasound Mode *(All products)*

*Replacing Peripherals Pairing Ultrasound Volume Model*

Cameras Camera[1..2] Focus Mode *(MX700, MX800)*

*Added for the integrated cameras*

Cameras SpeakerTrack Whiteboard Mode *(Codec Plus, Room Kit, Room 55)*

Macros AutoStart *(All products except SX10)*

Macros Mode *(All products except SX10)*

NetworkServices HTTP Proxy Allowed *(All products)*

NetworkServices HTTP Proxy LoginName *(All products)*

NetworkServices HTTP Proxy Mode *(All products)*

NetworkServices HTTP Proxy Password *(All products)*

NetworkServices HTTP Proxy Url *(All products)*

RTP Video Ports Range Start *(All products)*

RTP Video Ports Range Stop *(All products)*

Security Session FailedLoginsLockoutTime *(All products)*

Security Session MaxFailedLogins *(All products)*

UserInterface CustomMessage *(All products)*

UserInterface OSD HalfwakeMessage *(All products)*

UserInterface SettingsMenu Mode *(All products)*

Video Input Connector[n] HDCP Mode *(Room 55)*

### Configurations that are removed

Conference MultiStream Mode *(SX10, DX70, DX80)*

Peripherals Pairing Ultrasound Volume MaxLevel *(All products)*

*Replaced by Audio Ultrasound MaxVolume*

Peripherals Pairing Ultrasound Volume Mode *(All products)*

*Replaced by Audio Ultrasound Mode*

### Configurations that are modified

Audio Input MicrophoneMode *(DX70, DX80)*

**OLD:** User role: ADMIN

**NEW:** User role: ADMIN, INTEGRATOR

Audio Input Microphone[n] Level *(Room Kit, Room 55)*

**OLD:** Value space: 0..36

**NEW:** Value space: 0..26

Cameras Camera[n] Focus Mode *(SX80, MX700, MX800, Codec Plus)*

**OLD:** Value space: Auto/Manual

**NEW:** Value space: Auto/AutoLimited/Manual

Cameras SpeakerTrack Closeup *(SX80, MX700, MX800, Room Kit, Codec Plus, Room 55)*

**OLD:** User role: ADMIN, INTEGRATOR

**NEW:** User role: ADMIN, INTEGRATOR, USER

Cameras SpeakerTrack Whiteboard Mode *(SX80, MX700, MX800)*

**OLD:** User role: ADMIN, INTEGRATOR

**NEW:** User role: ADMIN, INTEGRATOR, USER

Security Audit Logging Mode *(All products)*

**OLD:** Default value: Off

**NEW:** Default value: Internal

UserInterface Language *(All products)*

**NEW:** Arabic and Hebrew added to valuespace



UserInterface OSD Output *(Room Kit)*

OLD: Default value: 1

NEW: Default value: Auto

Video Input Connector[2] Name *(Codec Plus, Room 55)*

OLD: Default value: PC (HDMI1)

NEW: Default value: PC 1 (HDMI)

Video Input Connector[3] Name *(Codec Plus, Room 55)*

OLD: Default value: PC (HDMI2)

NEW: Default value: PC 2 (HDMI)

Video Output Connector[1] Resolution *(MX200G2, MX300G2, DX70, DX80, Room 55)*

OLD: User role: ADMIN, INTEGRATOR

NEW: User role: ADMIN, INTEGRATOR, USER

Video Selfview OnCall Mode *(Room Kit)*

OLD: Default value: Off

NEW: Default value: On

## Codec Plus at a glance

Cisco Webex Codec Plus, is a powerful collaboration solution that integrates well with flat panel displays through HDMI CEC. The codec is rich in functionality and easily scalable to all of your conference rooms and spaces.

The Codec Plus is built for both cloud (Cisco Webex) and on-premise (CUCM and VCS) deployments. Cisco offers Codec Plus in the following bundles, ideal for medium to large-sized meeting rooms:

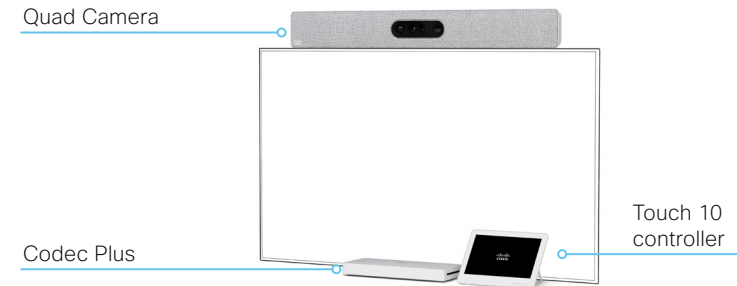
- *Cisco Webex Room Kit Plus* with Codec Plus, Quad Camera and Touch 10 user interface. External microphones are required. The Quad Camera has integrated loudspeakers and integrated microphones for speaker tracking; it detects meeting participants and shows the best overview; it detects and switches between active speakers (speaker tracking).
- *Cisco Webex Room Kit Plus Precision 60* with Codec Plus, Precision 60 camera and Touch 10 user interface. External microphones and loudspeakers are required.
- *Cisco Webex Room Kit Plus PTZ-12* with Codec Plus, PTZ-12 camera and Touch 10 user interface. External microphones and loudspeakers are required.

## Features and benefits

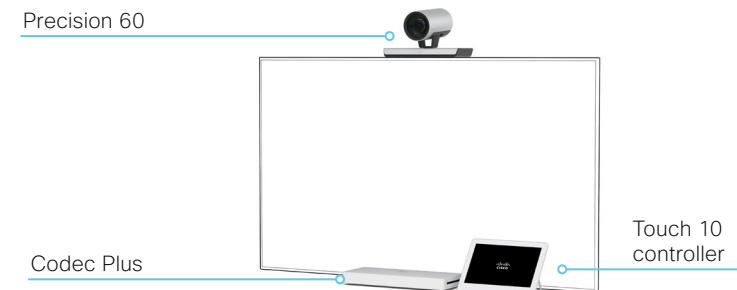
- Automatic wake-up feature, detecting when someone walks into the room
- Can recognize people through their mobile device when the Webex app is installed
- Controlled by Cisco Touch 10, or with a Cisco Webex app-enabled device
- Supports two displays for video and content
- Presentation of two content sources in local meetings
- 4K content sharing (30 fps in local meetings; 5 fps when sharing with far-end)
- Wired or wireless content sharing
- Counts people in the room, enabling analytics for better resource planning
- Ethernet and Wi-Fi support
- Controls peripherals such as lights and blinds through the Cisco Touch 10 (in-room control)
- Supports HDCP content for local viewing

See the datasheet for more information:  
 ▶ <https://www.cisco.com/go/roomkit>

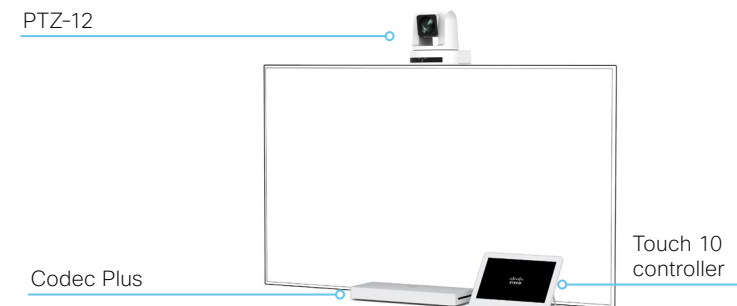
Cisco Webex Room Kit Plus



Cisco Webex Room Kit Plus Precision 60



Cisco Webex Room Kit Plus PTZ-12

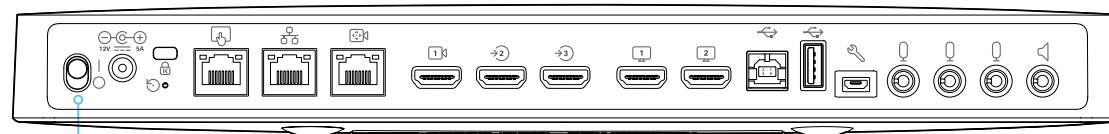


## Power On and Off (page 1 of 2)

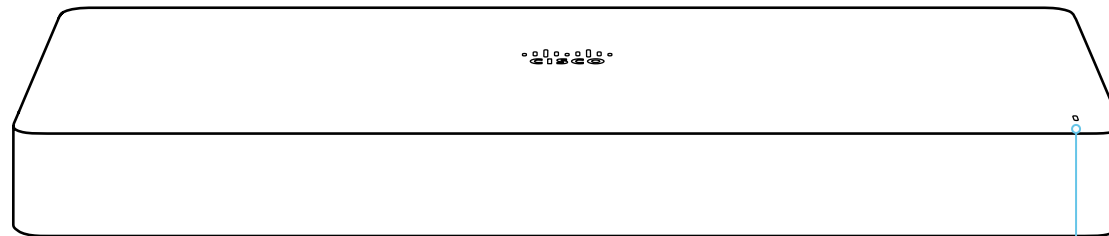
### Power On/Off with the Power switch

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

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



Power switch



LED

## Power On and Off (page 2 of 2)

### Restart and standby using the user interface

#### Restart the device

1. Select the device name or address at the top of the user interface.
2. Select [Settings](#), followed by [Restart](#).
3. Select [Restart](#) again to confirm your choice.

#### Enter standby mode

1. Select the device name or address at the top of the user interface.
2. Select [Standby](#).

#### Exit standby mode

- Tap the screen of the Touch controller.

### Power Off or restart the device remotely

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

#### Restart the device

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

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

#### Power Off the device

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



You cannot power the device on again remotely.

For the device to power up after a remote shutdown, turn the power switch Off and then On.

## LED indicators



### LED behavior

*In idle mode (screens are awake):*

Steady light.

*In standby mode (screens are off):*

Steady light.

*In sleep mode (low power mode):*

The LED pulsates slowly.

*The device needs attention (e.g. no network connection):*

The LED repeatedly flashes twice.

*During startup (boot):*

The LED flashes. It turns steady when the device is ready for use.

## How to administer the video conferencing device (page 1 of 4)

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

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

- HTTP/HTTPS (also used by the web interface)
- WebSocket
- SSH
- Serial connection

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

### 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 statuses are available in the web interface than in the API.

Access method	Notes	How to enable/disable the methods
<b>HTTP/HTTPS</b>	<ul style="list-style-type: none"> <li>• Used by the web interface of the device</li> <li>• Non-secure (HTTP) or secure (HTTPS) communication</li> <li>• HTTPS: <i>Enabled</i> by default</li> <li>• HTTP: <i>Enabled</i> by default only for devices that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the device has not been factory reset after the upgrade</li> </ul>	<p><a href="#">NetworkServices &gt; HTTP &gt; Mode</a></p> <p>Restart the device for changes to take effect</p>
<b>WebSocket</b>	<ul style="list-style-type: none"> <li>• Tied to HTTP, so that also HTTP or HTTPS must be enabled before you can use WebSocket</li> <li>• Encrypted (wss) or unencrypted (ws) communication</li> <li>• <i>Disabled</i> by default</li> </ul>	<p><a href="#">NetworkServices &gt; HTTP &gt; Mode</a></p> <p><a href="#">NetworkServices &gt; WebSocket</a></p> <p>Restart the device for changes to take effect</p>
<b>SSH</b>	<ul style="list-style-type: none"> <li>• Secure TCP/IP connection</li> <li>• <i>Enabled</i> by default</li> </ul>	<p><a href="#">NetworkServices &gt; SSH &gt; Mode</a></p> <p>You do not need to restart the device. It may take some time for changes to take effect</p>
<b>Serial connection</b>	<ul style="list-style-type: none"> <li>• Connect to the device 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>	<p><a href="#">SerialPort &gt; Mode</a></p> <p>Restart the device for changes to take effect</p>



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

How to administer the video conferencing device (page 2 of 4)

## The web interface of the device

The web interface is the administration portal for the device. You can connect from a computer and administer the device 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.

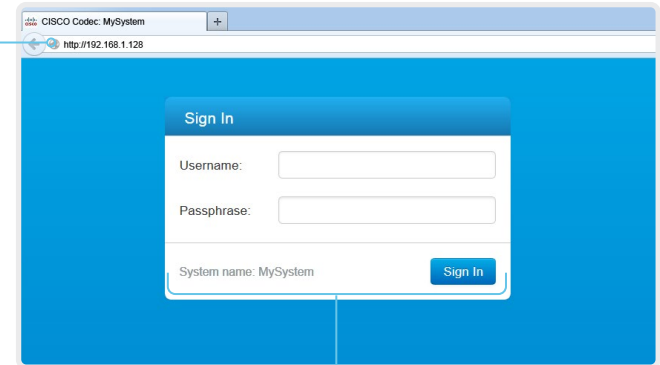
### Connect to the device

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



#### How to find the IP address

1. Select the device name or address at the top of the user interface.
2. Select [Settings](#), followed by [About this device](#).



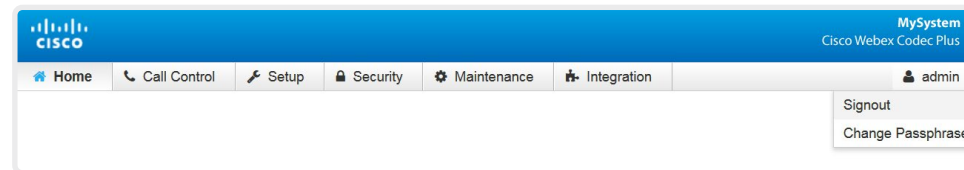
### Sign in

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



The device 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.

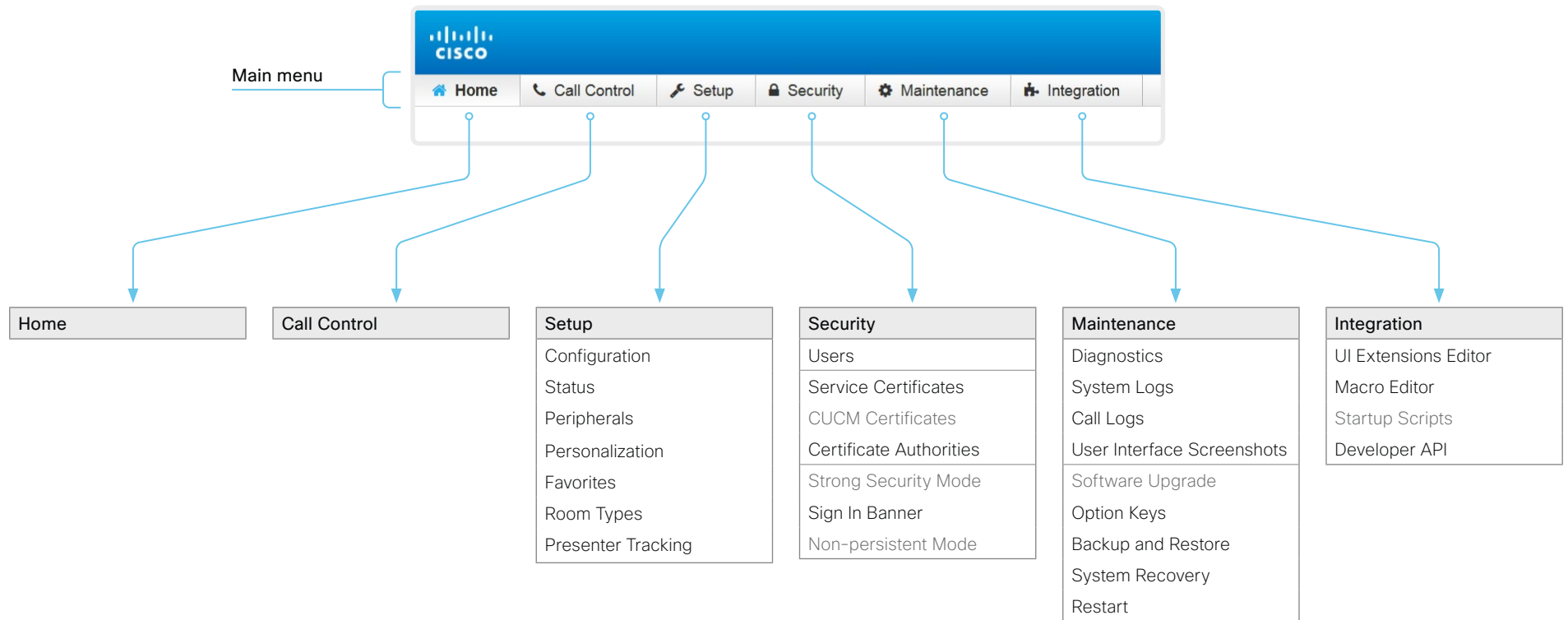
How to administer the video conferencing device (page 3 of 4)

## How the web interface is organized

The web interface is organized in sub-pages. All sub-pages shown below are available if the device is registered to an on-premise service (CUCM, VCS); the pages shown in grey color are not available if the device is registered to the Cisco cloud service (Cisco Webex).

In both cases, 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 conferencing device (page 4 of 4)

## Settings and device information on the user interface

You have access to device information, and some basic configurations and device tests on the device's user interface.

Device-critical settings and functions, such as network settings, service activation, and factory reset, may be protected by a passphrase, refer to the ► [Restrict the access to the Settings menu](#) chapter.

Some of the settings and tests are also part of the *Setup assistant* that is launched when the device is powered up for the first time. The Setup assistant is described in the *Getting Started Guide* for devices running CE software.

### Access Settings

1. Select the device name or address at the top of the user interface.
2. Select *Settings*.

A padlock symbol  indicates that a setting is protected (locked down).

3. Select the setting you want to change, or the test you want to run.

If a setting is locked down, an authentication window pops up, and you have to sign in with ADMIN credentials to proceed.

## Chapter 2

# Configuration

## User administration

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

### The default user account

The device 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 device 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 [Edit 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.

### 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.

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

**ROOMCONTROL:** A user with this role can create customized UI panels (for example in-room controls). The user has access to the UI Extensions editor and corresponding development tools.

**INTEGRATOR:** A user with this role has access to settings, commands and status that are required to set up advanced AV scenarios, and to integrate our devices with 3<sup>rd</sup> party equipment. Such a user can also create customized UI panels.

## Change the device passphrase

You need to know the device passphrase in order to:

- Sign in to the web interface
- Sign in and use the command line interfaces

### The default user account

The device 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 device configuration. It is also mandatory to set a passphrase for any other user with ADMIN rights.

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

### Other user accounts

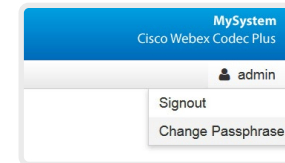
You can create many user accounts for the device.

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.

## Restrict the access to the Settings menu

By default, any user has access to the Settings menu on the user interface .

We recommend that you restrict the access to prevent unauthorized users from changing the configuration of the device.

### Lock down the Settings menu

1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Go to [UserInterface > SettingsMenu > Mode](#), and select **Locked**.
3. Click [Save](#) for the change to take effect.

Now a user has to sign in with ADMIN credentials to get access to the device-critical settings on the user interface (Touch controller).

### Unlock the Settings menu

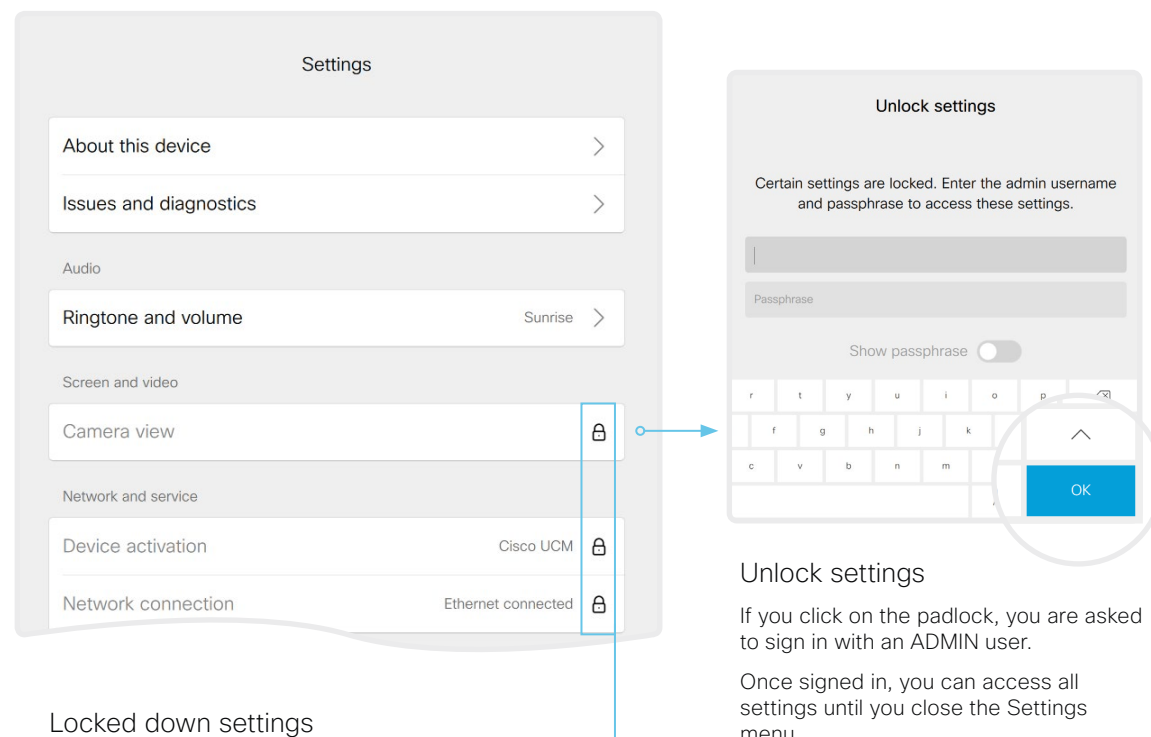
1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Go to [UserInterface > SettingsMenu > Mode](#), and select **Unlocked**.
3. Click [Save](#) for the change to take effect.

Now any user has access to the complete Settings menu on the user interface (Touch controller).

### The Settings menu on the user interface

If the menu is locked down, you must sign in to access the device-critical settings.

Select the *device name* or address at the top of the user interface followed by [Settings](#), in order to open the Settings menu.



### Locked down settings

Locked down settings are marked with a padlock.

### Unlock settings

If you click on the padlock, you are asked to sign in with an ADMIN user.

Once signed in, you can access all settings until you close the Settings menu.

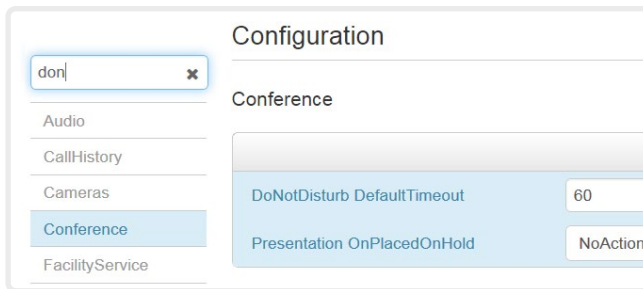
## Device configuration

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

### Find a device setting

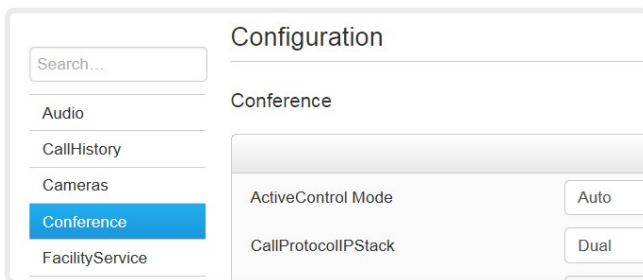
#### Search for settings

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



#### Select a category and navigate to settings

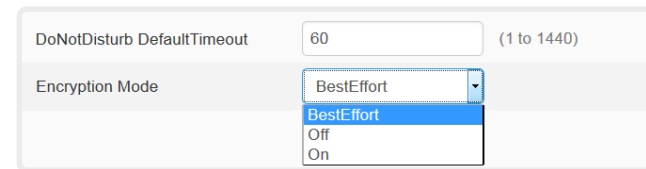
The device settings are grouped in categories. Choose a category in the left pane to show the associated settings.



### Change a device setting

#### Check the value space

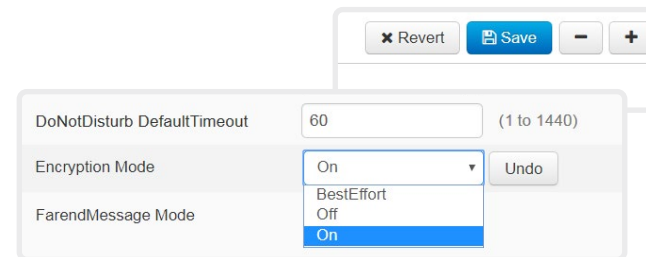
A settings's value space is specified either by text following the input field or in a drop-down list that opens when you click the arrow.



#### Change a value

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

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



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

### About device settings

All device settings can be changed from the web interface.

Each device setting is described in the [Device settings](#) chapter.

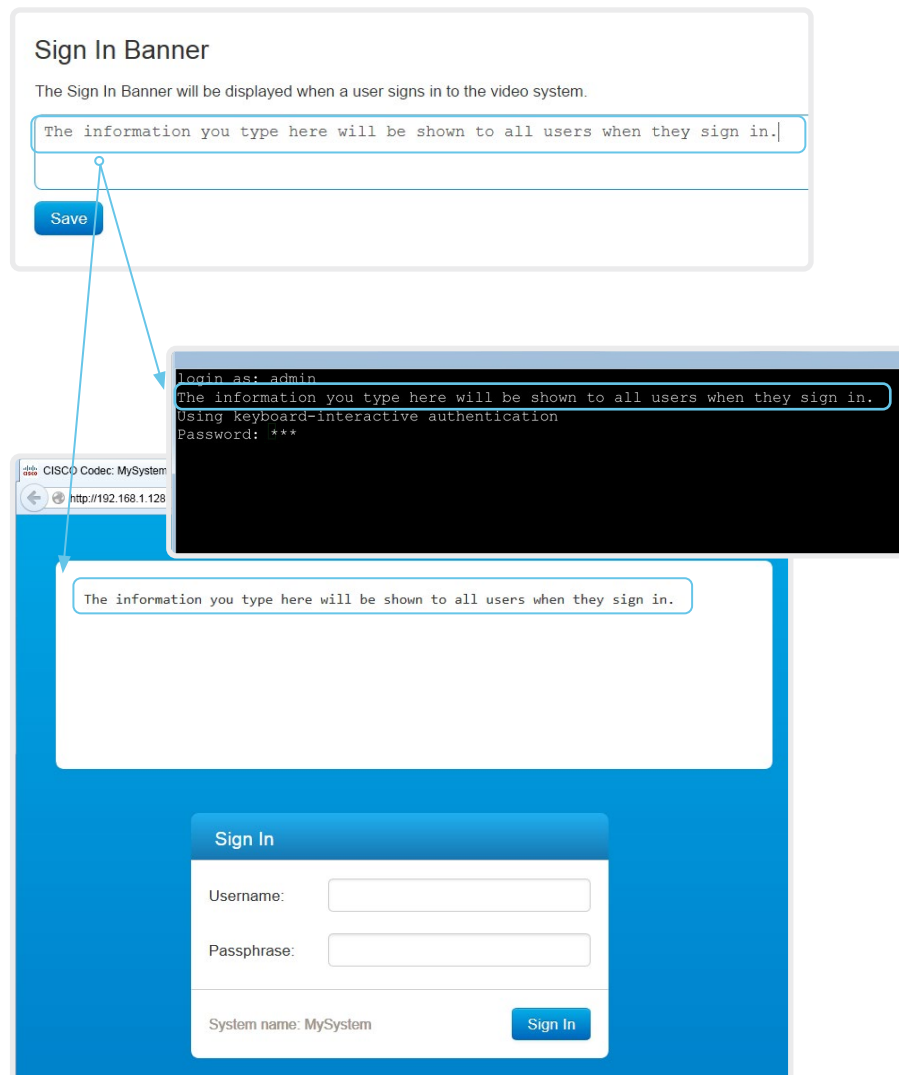
Different settings may require different user credentials. In order to be sure that an administrator is able to change all device settings, an administrator user must possess all user roles.

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 device 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.

The maximum size is: 4kByte

### Welcome banner versus sign in banner

Sign in banner:

- The banner is shown *before* the user signs in to the web interface or the command line interface.

Welcome banner:

- The banner is shown *after* the user has signed in to the web interface or the command line interface.

## Add a welcome banner

Adding a Welcome banner is only available using API commands; we don't provide a dedicated user interface for it.

### API commands

```
xCommand SystemUnit WelcomeBanner Set
```

This is a multiline command. Anything you input after you issue the command, is input to the command (including line breaks). Finish the input with a separate line containing just a period ending with a line break.

There are also a few more welcome banner commands, refer to the API-guide for more details.

```
xCommand SystemUnit WelcomeBanner Clear
```

```
xCommand SystemUnit WelcomeBanner Get
```

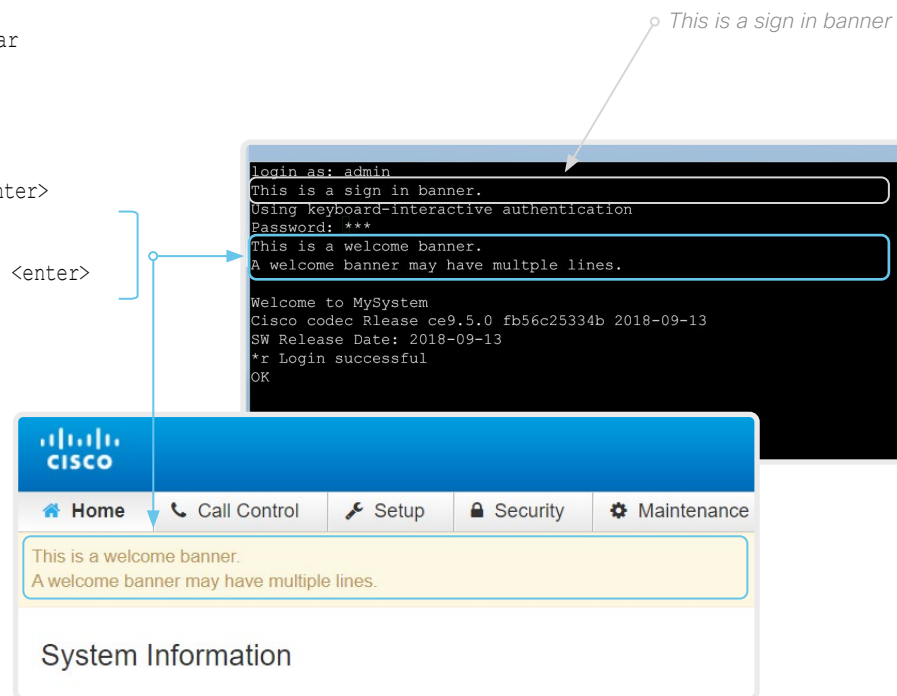
### Example

```
xCommand SystemUnit WelcomeBanner Set <enter>
```

```
This is a welcome banner. <enter>
```

```
A welcome banner may have multiple lines. <enter>
```

```
. <enter>
```



### About welcome banner

You can set up a welcome banner that users see after they sign in to the device's web interface or command line interface. The banner can have multiple lines.

The banner can for example contain information you need in order to get started, or things you must be aware of when setting up the device.

The maximum size is: 4 kByte

### Welcome banner versus sign in banner

Sign in banner:

- The banner is shown *before* the user signs in to the web interface or the command line interface.

Welcome banner:

- The banner is shown *after* the user has signed in to the web interface or the command line interface.



## Manage the service certificates of the device

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 device.

### About the service certificates of the device

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

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

The device's certificates are text files that verify the authenticity of the device. 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 device, 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.

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

**Add Certificate**

Certificate  No file selected.

Private key (optional)  No file selected.

Passphrase (optional)

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

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

### Add a certificate

1. Browse to 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 device.
- Only certificates with a validity period of up to 10 years are accepted.

## Manage the lists of trusted certificate authorities - CAs (page 1 of 4)

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

You can configure the device to demand that a server or client presents its certificate before communication is set up. The device uses the certificate to verify the authenticity of the server or client. If authentication fails, the connection will not be established.

The certificate (text file) must be signed by a trusted Certificate Authority (CA). Lists of certificates from trusted CAs reside on the device.

### The CA certificate lists

You can check and maintain the lists of trusted CAs from the web interface of the device:

- Sign in to the web interface, navigate to [Security > Certificate Authorities](#). There is one tab for each CA list.

These are the CA lists:

- [Preinstalled](#): Pre-installed CA certificates that are used to validate the certificates of external servers (HTTPS, syslog) that the device communicates with.
- [Collaboration Edge](#): Pre-installed CA certificates that are used to validate the certificates of servers contacted over the Internet when the device is provisioned by Cisco Unified Communications Manager (CUCM) via Expressway (also known as MRA or Edge).
- [Custom](#): CA certificates that you have uploaded to the device yourself. The list must include all CAs that are needed in order to verify certificates for both logging and other connections, if those certificates are not already included in the pre-installed lists.

Manage the lists of trusted certificate authorities - CAs (page 2 of 4)

## Manage pre-installed CA certificates for external servers

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

**Certificate Authorities**

Custom Preinstalled Collaboration Edge

This CA list is used to validate the certificates of external servers that the video device communicates with:

- HTTP servers hosting content used by the `HttpClient` xAPI, Macros, etc.
- SMTP mail servers (applies to Webex Boards only)

Certificate	Issuer		
Certificate_01	Issuer_1	Details...	Disable
Certificate_02	Issuer_2	Details...	Disable
Certificate_03	Issuer_3	Details...	Disable
Certificate_04	Issuer_4	Details...	Disable

Disable All

### View or disable certificates

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

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

Refer to the [Upload a CA certificate to the device](#) chapter how to update the list of trusted CA certificates.

### Pre-installed CA certificates

A list of commonly used CA certificates is pre-installed on the device. The device uses this list when validating certificates from external servers that it communicates with:

- HTTP servers that host content used by the `HttpClient` API or macros
- Provisioning servers
- Phone book servers
- Syslog servers (for external logging)
- Servers and services used by the Cisco Webex cloud

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

Manage the lists of trusted certificate authorities - CAs (page 3 of 4)

## Manage pre-installed CA certificates for CUCM via Expressway provisioning

Sign in to the web interface, navigate to [Security > Certificate Authorities](#), and open the [Collaboration Edge](#) tab.

**Certificate Authorities**

Custom Preinstalled Collaboration Edge

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

Configure provisioning now.

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

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

Disable All

### View or disable certificates

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

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

Refer to the [Upload a CA certificate to the device](#) chapter how to update the list of trusted CA certificates.

### Pre-installed CA certificates for CUCM via Expressway

The pre-installed CA certificates in this list are only used when the device 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 device will not be provisioned and registered.

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

Manage the lists of trusted certificate authorities - CAs (page 4 of 4)

## Upload a CA certificate to the device

Sign in to the web interface, navigate to [Security > Certificate Authorities](#), and open the [Custom](#) tab.

You need the following file:

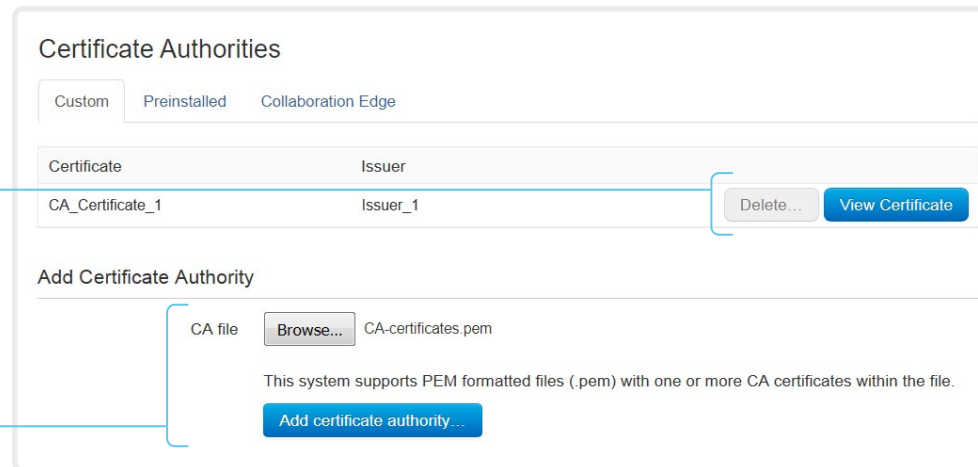
- CA certificate list (file format: .PEM).

### View or delete a certificate

Use the corresponding button to view or delete a certificate.

### Upload a list of CA certificates

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



The certificates and certificate issuers in the illustration are examples. Your device 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 the custom list of trusted CA certificates

This list contains the CA certificates that you have uploaded to the device yourself. They can be used to validate client and server certificates for both logging and other connections.

They can be used for:

- HTTP servers that host content used by the HttpClient API or macros
- Provisioning servers
- Phone book servers
- SIP servers
- Syslog servers (for external logging)
- Cisco Expressway infrastructure
- Servers and services used by the Cisco Webex cloud

## Set up secure audit logging

Sign in to the web interface and navigate to *Setup > Configuration*.



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

Refer to the [Upload a CA certificate to the device](#) 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.
3. Set *Audit > Logging > Mode* to **ExternalSecure**.
4. Click *Save* for the change to take effect.

The screenshot shows the 'Configuration' page for 'Security'. The 'Audit' section is expanded, showing the following settings:

- Logging Mode:** ExternalSecure (dropdown menu with options: ExternalSecure, External, Internal, Off)
- OnError Action:** ExternalSecure (dropdown menu with options: ExternalSecure, Internal, Off)
- Server:**
  - Address:** (text input field)
  - Port:** 514 (text input field)
  - PortAssignment:** Auto (dropdown menu)

Buttons for 'Revert', 'Save', and zoom controls are visible at the top right of the configuration area.

### About secure audit logging

When audit logging is enabled, all sign in activity and configuration changes on the device 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 device 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 list of pre-installed CA certificates or the custom CA list.

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


## Delete CUCM trust lists

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

Sign in to the web interface and 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 device.

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

### Change the persistency settings

All persistency settings are set to **Persistent** by default. You only have to change these settings if you want 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 restart...](#)

The device 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 device 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 device restarts:

- Device 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 device to delete such information.

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



## Set strong security mode

Sign in to the web interface and 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 device restarts automatically.

2. Change the passphrase when you are prompted. The new passphrase must meet the strict criteria as described.

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

### Return to normal mode

Click [Disable Strong Security Mode...](#) in order to restore the device to normal mode. Confirm your choice in the dialog box that appears.

The device 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.

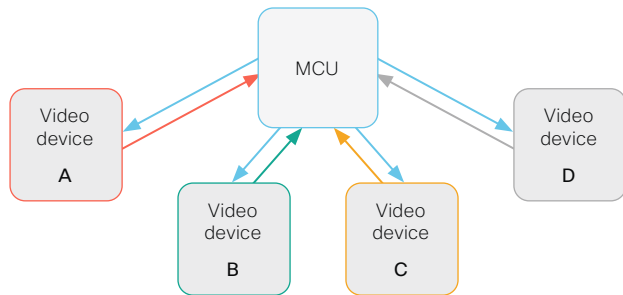
Strong security mode sets very strict passphrase requirements, and requires all users to change their passphrase on the next sign in.

## Set up ad hoc multipoint conferences (page 1 of 2)

There are several ways to expand a point-to-point video call (a call involving only two parties) into a multipoint conference with more participants.

### Centralized conference infrastructure

Most solutions are based on a centralized conference infrastructure, i.e. an MCU (multipoint control unit) <sup>1</sup>.

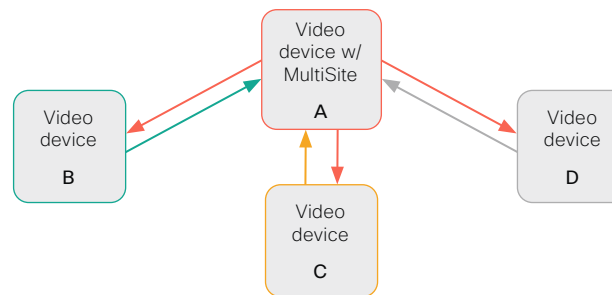


In this set-up video devices A, B, C and D participates in a 4-party conference. The MCU receives media streams from all the devices, processes the streams, and sends all media to the other participants.

### Local conference resources - MultiSite

*(not available for SX10, DX70, and DX80)*

In a MultiSite scenario, one of the video devices has MCU functionality.



In this set-up video devices A, B, C and D participates in a 4-party conference. Device A uses its MultiSite functionality and acts as an MCU. It receives media streams from all the devices, processes the streams, and sends all media to the other participants.

MultiSite is not part of the standard product delivery; you must buy an upgrade option to get the *MultiSite option key* installed on the device.

The maximum number of participants supported by MultiSite is:

- SX10, DX70, and DX80: No MultiSite support
- SX80, MX700, and MX800: Five participants (yourself included) plus one additional audio call
- Codec Pro, Room 70 G2: Five participants (yourself included)
- Other products: Four participants (yourself included)

### Multipoint configuration

Use the [Conference > Multipoint > Mode](#) setting to decide how to handle multipoint conferences. This setting takes the following values:

- Auto
- CUCMMediaResourceGroupList
- MultiSite *(not available for SX10, DX70, DX80)*
- Off *(not available for SX10, DX70, DX80)*

The table on the next page explains the different conferencing options.

<sup>1</sup> MCU - multipoint control unit, also called video-conferencing gateway or bridge.

## Set up ad hoc multipoint conferences (page 2 of 2)

Conference Multipoint Mode setting	MultiSite option key	Remote device type <sup>2</sup>	Add participant behavior
Off <sup>3</sup>	N/A	MCU	<ul style="list-style-type: none"> <li>Direct Remote Add</li> <li>If the MCU supports <i>Add Participant</i>, there is an <i>Add</i> button in the UI and you can call the next participant directly. The new participant is added to the conference as soon as he accepts the call.</li> <li>If the MCU does not support <i>Add Participant</i>, there is no <i>Add</i> button in the UI.</li> </ul>
		Video device	<ul style="list-style-type: none"> <li>Plus one audio</li> <li>You can add one extra participant on audio-only.</li> <li>You cannot add more participants on video.</li> </ul>
CUCM-MediaResource-GroupList	N/A	Video device	<ul style="list-style-type: none"> <li>Consultative Add</li> <li>Available only to CUCM registered devices, and the <i>SIP Type</i> setting must be <b>Cisco</b>.</li> <li>The conference is put on hold while calling a new participant. When the new participant accepts the call you can merge the new call with the conference.</li> <li>Only the participant who added the first new participant to the conference can add more participants.</li> </ul>
MultiSite <sup>3</sup>	Yes	N/A	<ul style="list-style-type: none"> <li>Local Multisite <sup>4</sup></li> <li>There is an <i>Add</i> button in the UI, and you can call the next participant directly.</li> <li>You can keep adding participants until you reach the maximum number for the device.</li> </ul>
	No	N/A	<ul style="list-style-type: none"> <li>Plus one audio</li> <li>You can add one extra participant on audio-only.</li> <li>You cannot add more participants on video.</li> </ul>
Auto	Yes	MCU	<ul style="list-style-type: none"> <li>Direct Remote Add</li> <li>If the MCU supports <i>Add Participant</i>, there is an <i>Add</i> button in the UI and you can call the next participant directly. The new participant is added to the conference as soon as he accepts the call.</li> <li>If the MCU does not support <i>Add Participant</i>, there is no <i>Add</i> button in the UI.</li> </ul>
		Video device	<ul style="list-style-type: none"> <li>Local Multisite without cascading <sup>4</sup></li> <li>There is an <i>Add</i> button in the UI, and you can call the next participant directly.</li> <li>You can keep adding participants until you reach the maximum number for the device.</li> <li>Only the MultiSite host (which is now acting as an MCU) can add participants. This prevents cascaded conferences.</li> </ul>
	No	MCU	<ul style="list-style-type: none"> <li>Direct Remote Add</li> <li>If the MCU supports <i>Add Participant</i>, there is an <i>Add</i> button in the UI and you can call the next participant directly. The new participant is added to the conference as soon as he accepts the call.</li> <li>If the MCU does not support <i>Add Participant</i>, there is no <i>Add</i> button in the UI.</li> </ul>
		Video device	<ul style="list-style-type: none"> <li>Plus one audio</li> <li>You can add one extra participant on audio-only (not supported for SX10, DX70, and DX80).</li> <li>You cannot add more participants on video.</li> </ul>

<sup>2</sup> The remote device type is shown in the *Call [n] DeviceType* status.

<sup>3</sup> Not supported for SX10, DX70, and DX80.

<sup>4</sup> We recommend setting *Conference Multipoint Mode* to **Auto** rather than to **MultiSite** in order to avoid cascaded conferences.

## 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 mobile device is close to a video conferencing device.

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



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

Video conferencing device	Maximum number of connections
Room Kit, Room Kit Mini	30 / 7 *
Room 55, Room 55 Dual, Room 70, Room 70 G2	30 / 7 *
Codec Plus, Codec Pro	30 / 7 *
Board 55/55S, Board 70/70S, Board 85S	30 / 7 *
SX80	10
SX10, SX20	7
MX700, MX800	10
MX200 G2, MX300 G2	7
DX70, DX80	3

\* 30 connections when the *View shared content on a mobile device* service is disabled; 7 connections when this service is enabled.

### Proximity services

*Place calls and control the video conferencing device:*

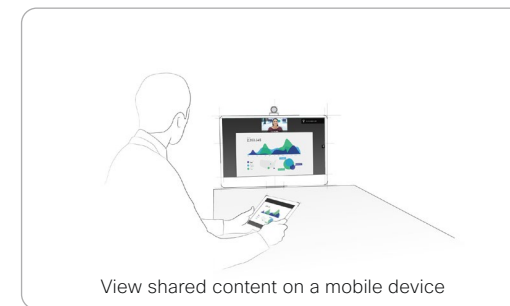
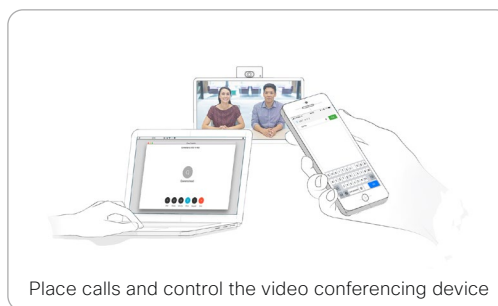
- Dial, mute, adjust volume, hang up
- Available on laptops (OS X and Windows), smartphones and tablets (iOS and Android)

*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 laptop:*

- 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 ► <https://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, ► [https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN\\_.html](https://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 conferencing devices emit ultrasound pairing messages as part of the Proximity feature.

Use the [Proximity > Mode](#) setting to switch the Proximity feature - and thereby also emission of ultrasound pairing messages - **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.

*Room 70, Room 70 G2, Room 55, Room 55 Dual, Room Kit, Room Kit Mini, Room Kit Plus, 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.

*Boards:*

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

For Board 50 and 70 (not *S Series*) the level can be slightly higher right below the screen due to the downward-facing loudspeakers.

*Codec Plus, Codec Pro, SX10, SX20, and SX80:*

- We cannot foresee the ultrasound sound pressure level on these video conferencing devices, because they emit ultrasound on third-party loudspeakers.

The volume control on the loudspeaker itself, and the [Audio > Ultrasound > MaxVolume](#) 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 devices because:

- DX70 and DX80 have dedicated headset outputs, on which we never emit ultrasound.
- SX10N plays ultrasound on the built-in loudspeakers. Ultrasound is never emitted on the HDMI or audio outputs.

*Room 70, Room 70 G2, Room 55 Dual, Room Kit Plus, Codec Plus, Codec Pro, Boards, SX10, SX20, SX80, and MX Series:*

- These devices are not designed for headset use.
- We strongly recommend you to switch off ultrasound emission if you use a headset with these video conferencing devices (set [Proximity > Mode](#) to **Off**). Then you *cannot* use the Proximity feature.
- Since these devices don't have dedicated headset outputs, we are not able to control the sound pressure level from the connected headsets.

*Room 55, Room Kit, Room Kit Mini:*

- You can always connect a headset to the *USB output* of these devices, because we don't emit ultrasound on this output.
- The *audio line outputs (mini-jack)* of the Room 55 and Room Kit are **not** designed for headset use. We are not able to control the sound pressure level from a headset that is connected to one of these outputs..

If you connect a headset to an audio line output, we strongly recommend you to switch off ultrasound emission (set [Proximity > Mode](#) to **Off**). Then you *cannot* use the Proximity feature.

## 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 conferencing device starts sending ultrasound pairing messages.

Enable the services you want to allow. Only *Wireless share from a desktop client* 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 conferencing device:*

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

*View shared content on a mobile device:*

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

*Wireless share from a desktop client:*

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

### The Proximity indicator



You can see the Proximity indicator on the screen as long as at least one Proximity client is paired with the device.

The indicator doesn't disappear immediately when the last client unpairs. It may take a few minutes.

### 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 [Audio > Ultrasound > MaxVolume](#) setting.

When Proximity is switched **On**, the video conferencing device 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.

---

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

## 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 conferencing device 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:  
▶ <https://www.cisco.com/web/siteassets/legal/privacy.html>

### Basic troubleshooting

#### Cannot detect devices with Proximity clients

- Check if the video conferencing device is in standby mode. Ultrasound is not transmitted if the speakers (for example a TV in standby mode) are turned off.
- Check the speaker volume. The volume control on a speaker itself (not the volume controlled 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.
- 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.
- Check *Settings > Issues and diagnostics* on the user interface, or *Maintenance > Diagnostics* on the web interface of the video conferencing device. If there are no ultrasound related issues listed ("Unable to verify the ultrasound signal"), ultrasound pairing messages are emitted by the video conferencing device as they should. Refer to the Proximity *Support forum* for further assistance with the client detection issues.

#### Audio artifacts

- If you can hear audio artifacts, like humming or clipping noise, decrease the maximum ultrasound volume (*Audio > Ultrasound > MaxVolume*).

#### Cannot share content from a laptop

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

### Additional resources

Cisco Proximity site:

▶ <https://proximity.cisco.com>

Support forum:

▶ <https://www.cisco.com/go/proximity-support>



## Adjust the video quality to call rate ratio (page 1 of 2)

### Video input quality settings

When encoding and transmitting video there is a trade-off between high resolution (sharpness) and high frame rate (motion).

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.

### 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.

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

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

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**.
2. Go to [Video > Input > Connector n > OptimalDefinition > Profile](#) and choose the preferred optimal definition profile.

## Adjust the video quality to call rate ratio (page 2 of 2)

Resolutions and frame rate [w×h@fps] obtained for different optimal definition profiles and call rates						
Call rate [kbps]	H.264, maximum 30 fps			H.264, maximum 60 fps		
	<i>Normal</i>	<i>Medium</i>	<i>High</i>	<i>Normal</i>	<i>Medium</i>	<i>High</i>
128	320×180@30	320×180@30	512×288@30	320×180@30	512×288@20	512×288@30
256	512×288@30	640×360@30	768×448@30	512×288@30	640×360@30	768×448@30
384	640×360@30	768×448@30	768×448@30	640×360@30	768×448@30	768×448@30
512	768×448@30	1024×576@30	1024×576@30	768×448@30	1024×576@30	1024×576@30
768	1024×576@30	1280×720@30	1280×720@30	1024×576@30	1280×720@30	1280×720@30
1152	1280×720@30	1280×720@30	1280×720@30	1280×720@30	1280×720@30	1280×720@60
1472	1280×720@30	1280×720@30	1920×1080@30	1280×720@30	1280×720@30	1280×720@60
1920	1280×720@30	1920×1080@30	1920×1080@30	1280×720@30	1280×720@60	1280×720@60
2560	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1920×1080@60
3072	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1920×1080@60
4000	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1920×1080@60	1920×1080@60
6000	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60

Resolutions and frame rate [w×h@fps] obtained for different optimal definition profiles and call rates						
Call rate [kbps]	H.265, maximum 30 fps			H.265, maximum 60 fps		
	<i>Normal</i>	<i>Medium</i>	<i>High</i>	<i>Normal</i>	<i>Medium</i>	<i>High</i>
128	512×288@30	512×288@30	640×360@30	512×288@30	512×288@30	640×360@30
256	640×360@30	768×448@30	768×448@30	640×360@30	768×448@30	768×448@30
384	768×448@30	1024×576@30	1280×720@30	768×448@30	1024×576@30	1280×720@30
512	1024×576@30	1280×720@30	1280×720@30	1024×576@30	1280×720@30	1280×720@30
768	1280×720@30	1280×720@30	1920×1080@30	1280×720@30	1280×720@30	1280×720@60
1152	1280×720@30	1920×1080@30	1920×1080@30	1280×720@30	1280×720@60	1280×720@60
1472	1280×720@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1280×720@60
1920	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1920×1080@60
2560	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1920×1080@60	1920×1080@60
3072	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60
4000	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60
6000	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60

## Add corporate branding to the screen and Touch 10 user interface (page 1 of 2)

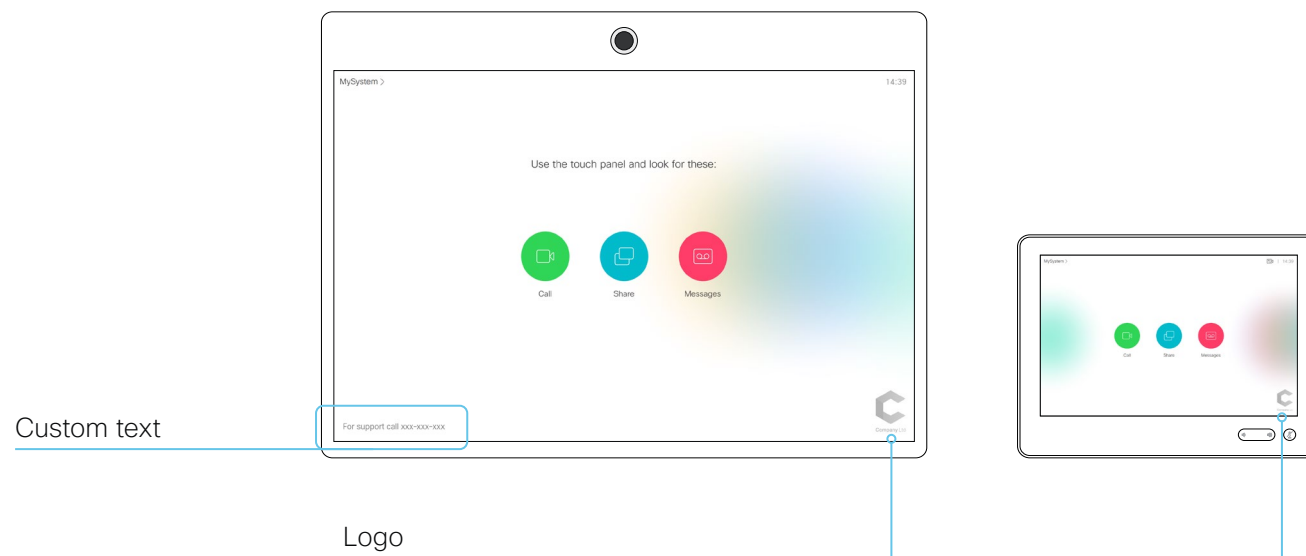
Sign in to the web interface, navigate to [Setup > Personalization](#), and open the [Branding](#) tab.

From this page you can add your own branding elements (background brand image, logo, custom message) to the video conferencing device.

### Branding in the awake state

In the awake state you can:

- Add a logo in the bottom right corner (screen and Touch 10)
- Add a short message (text only) in the bottom left corner (only on screen, not on Touch 10)



### Logo

We recommend:

- A black logo (the device will add a white overlay with 40% opacity so that the logo and the other user interface elements go well together)
- PNG-format with transparent background
- Minimum 272x272 pixels (it will be scaled automatically)

### About Branding

The Branding feature, as describe in this chapter, allows you to customize the screen and Touch user interface appearance without compromising the overall Cisco user experience.

We recommend that you use this feature rather than our legacy Custom wallpaper feature, which prevents the use of functionality such as One Button to Push.

**You cannot use the Branding feature and a Custom wallpaper at the same time.**

If your device is set up with a Custom wallpaper, you must click [Disable the custom wallpaper](#) before adding branding elements.

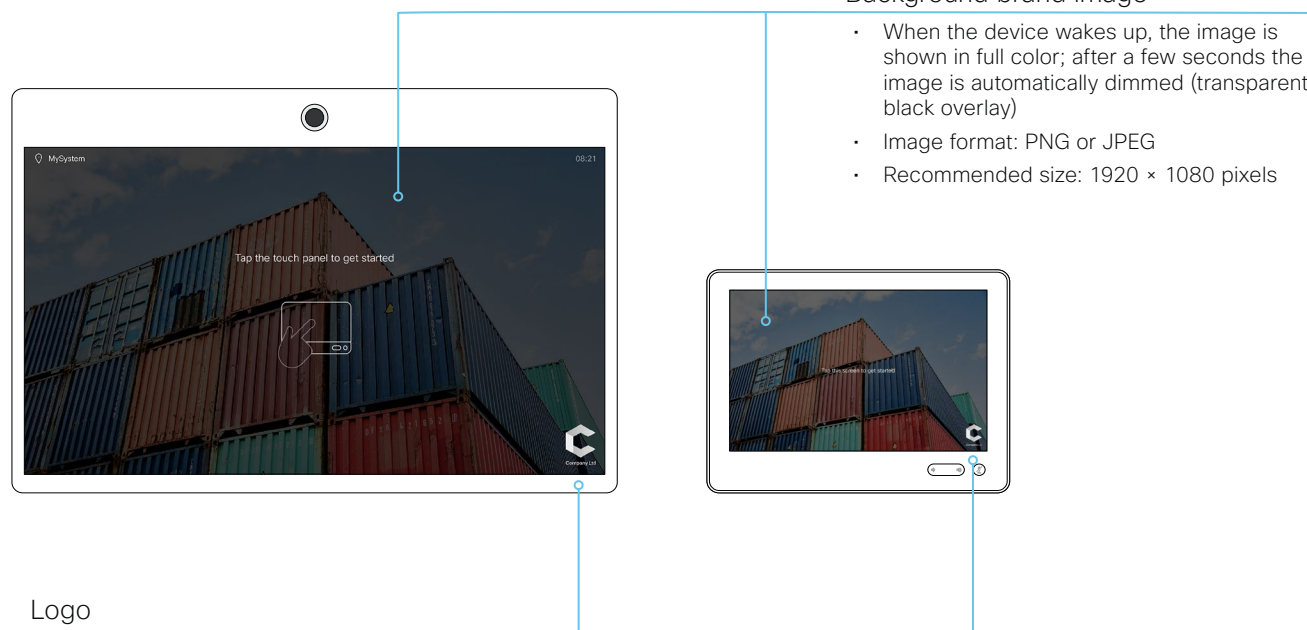
## Add corporate branding to the screen and Touch 10 user interface (page 2 of 2)

### Branding in the halfwake state

In halfwake state you can:

- Add a background brand image (screen and Touch 10)
- Add a logo in the bottom right corner (screen and Touch 10)
- Customize or remove the message at the center of the screen (only on screen, not on Touch 10). This is the message that informs the user how to start using the device

In general, we recommend that you keep the standard message. Change the message only if you have to adapt it to a different scenario, for example if you have a third-party user interface.



#### Background brand image

- When the device wakes up, the image is shown in full color; after a few seconds the image is automatically dimmed (transparent black overlay)
- Image format: PNG or JPEG
- Recommended size: 1920 × 1080 pixels

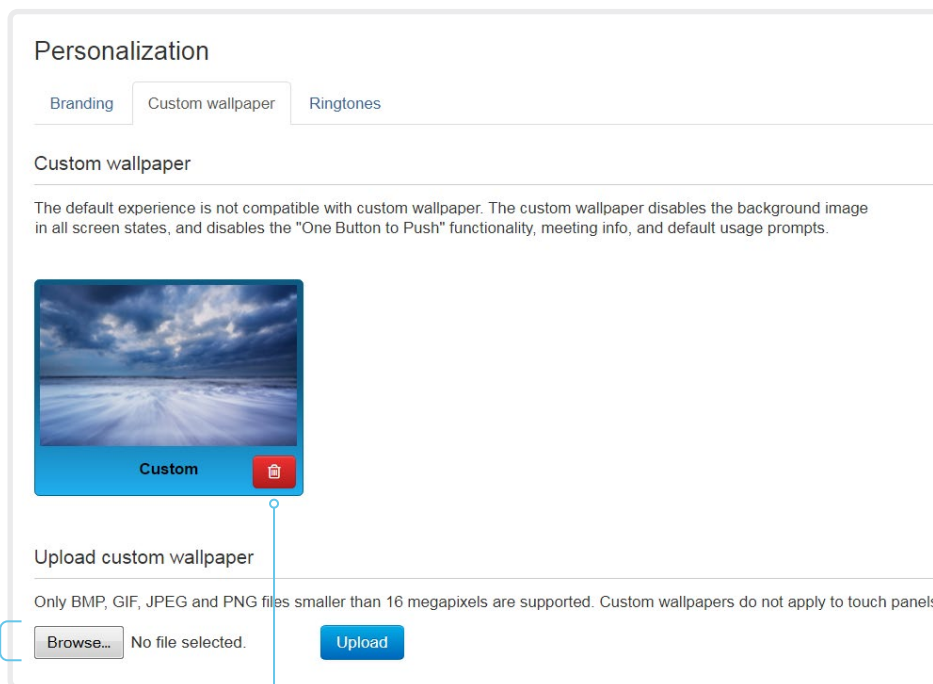
#### Logo

We recommend:

- A white logo (so that it goes well with the dark background brand image)
- PNG-format with transparent background
- Minimum 272×272 pixels

## Add a custom wallpaper

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



### Upload a custom wallpaper

Overwrites any old custom wallpaper.

1. Browse to find the custom wallpaper image file.
2. Click [Upload](#) to save the file on the device.

Supported file formats: BMP, GIF, JPEG, PNG

Maximum file size: 16 megapixels

The custom wallpaper is automatically activated once uploaded.

### Delete the custom wallpaper

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

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

### About a custom wallpaper

If you want a custom picture as background on your screen, you may upload and use a *custom wallpaper*. A custom wallpaper will not appear on the Touch controller.

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

We recommend that you use our new Branding feature rather than this legacy Custom wallpaper feature. You will get a better overall Cisco user experience, and avoid losing functionality such as One Button To Push and meeting information. See the [Add corporate branding to the screen and Touch 10 user interface](#) chapter.

**You cannot use the Branding feature and a Custom wallpaper at the same time.**

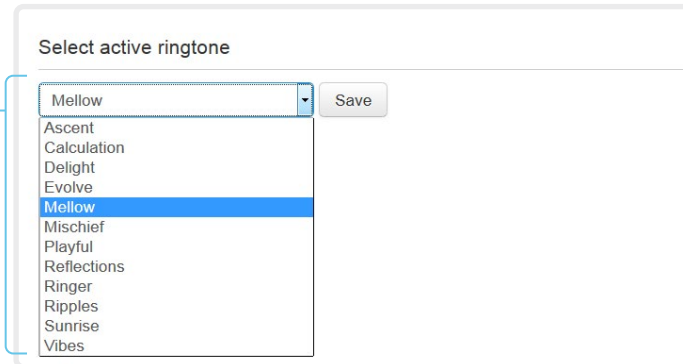
If your device is set up with branding elements you must click [Continue without branding](#) before adding a custom wallpaper.

## Choose a ringtone and set the ringtone volume

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

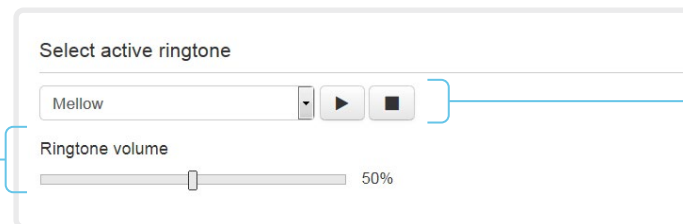
### Change the ringtone

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 is installed on the device. Use the web interface to choose a ringtone, and set the ringtone volume.

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

## Manage the Favorites list

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

### 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.

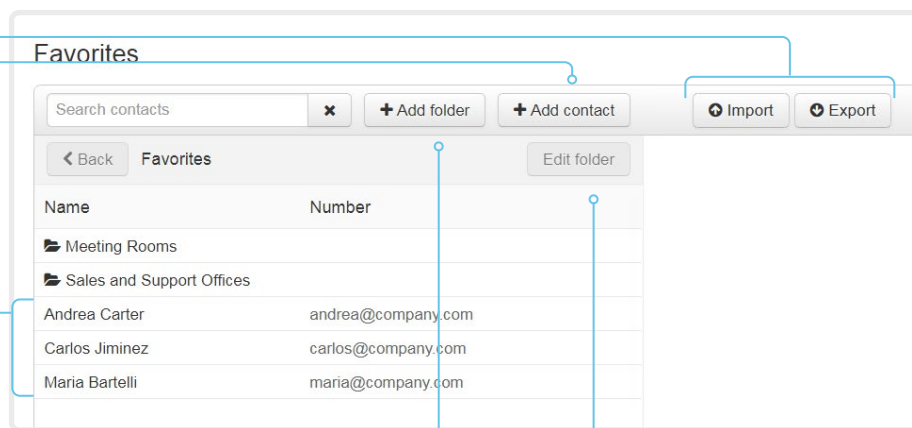
Choose a folder in the folder drop down list in order to store the contact in a sub-folder.

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 a folder's name followed by [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.

## Manage Favorites using the device's user interface

### Add a contact in the Favorites list

1. Select [Call](#) on the home screen.
2. Select the contact you want to add.
3. Select [Add to favorites](#).

The contact you add will be placed in the top folder. You cannot select or create a sub-folder.

### Remove a contact from the Favorites list

1. Select [Call](#) on the home screen.
2. Select the [Favorites](#) tab.
3. Select the contact you want to remove.
4. Select [Remove favorite](#).

## Set up accessibility features

### Flashing screen for incoming calls

To make it easier for the hearing impaired users to notice when someone is calling, the screen can be setup to flash red and gray on incoming calls.

1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Go to [UserInterface > Accessibility > IncomingCallNotification](#) and select **AmplifiedVisuals**.
3. Click [Save](#).



## Provisioning of product specific configurations from CUCM (page 1 of 2)

This chapter describes how to provision settings or parameters to a device (endpoint) using the method that was introduced in Cisco UCM Release 12.5(1)SU1.

Prior to Cisco UCM release 12.5(1)SU1, only a limited set of product-specific configurations were pushed from UCM to the device. The administrator had to rely on Cisco TMS or the web interface of the device to configure all the other settings.

From CUCM release 12.5(1)SU1 more settings or parameters can be provisioned from CUCM. The list of settings matches what users see on their device (public xConfigurations), with the exception of Network, Provisioning, SIP and H.323 settings.

For more information about CUCM refer to the *Video Endpoints Management* chapter of the [► Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5\(1\)SU1](#).

### Configuration control modes

Based on the deployment needs, administrators can configure various configuration control modes in the CUCM administration interface. You can decide whether you want to control the configuration settings from CUCM, the device, or both of them together.

These are the various configuration control modes:

- **Unified CM and Endpoint** (default): Use this mode if you want the CUCM and the device to operate as the multi-master source for provisioning device data. CUCM reads the xConfiguration data automatically from the device, and any updates made locally on the device is synchronised with the CUCM server instantly.
- **Unified CM:** CUCM operates as the centralized master source for provisioning device data. CUCM ignores any changes that are done locally on the device, and therefore such changes will be overridden the next time CUCM applies a new configuration to the device.
- **Endpoint:** The endpoint operates as the centralized master source of configuration data. In this mode, the endpoint ignores any configuration data from the CUCM and doesn't synchronize back the changes done locally.

This mode is typically used when an integrator is installing the devices and wants to control the configuration locally from the device.

### Pull configurations from the device on-demand

Administrators can use the [Pull xConfig. from Device](#) option in CUCM to pull configuration changes from the devices on-demand at any time.

This option is enabled only if the device is registered.

### Supported CE software versions

Any device that supports CE9.8 or higher can use this new provisioning layout in CUCM.

If the device has a software version prior to CE9.8, you will be able to view the complete set of parameters in the CUCM user interface; but you can only configure the subset that is marked with a "#". The "#" is to the right of each parameter value.

The full set of parameters functions only if you upgrade the device to CE9.8 or higher.

## Provisioning of product specific configurations from CUCM (page 2 of 2)

### Set up provisioning from CUCM

1. Sign in to CUCM, navigate to [Device > Phone](#), and find your device.
2. Find the *Product Specific Configuration Layout* section (see illustration).
3. Click the *Miscellaneous* category and find the *Configuration Control Mode* setting.  
Choose your preferred mode: Unified CM, Endpoint, or Unified CM and Endpoint (see the description on the previous page).
4. Click the [Pull xConfig. from Device](#) button if you want to load the current configuration from the device.
5. Select a category and set a value for the configurations you want to change.
6. Finally, click [Save](#) and [Apply Config](#), just like you do in earlier CUCM versions.

Pull configurations from the device on-demand

Click this button to pull any data configuration from the device on-demand.

Settings marked with a hash, #

Settings that also were available in Cisco UCM releases prior to 12.5(1) SU1.

Settings or parameters

The settings that belong to the selected category.

Categories

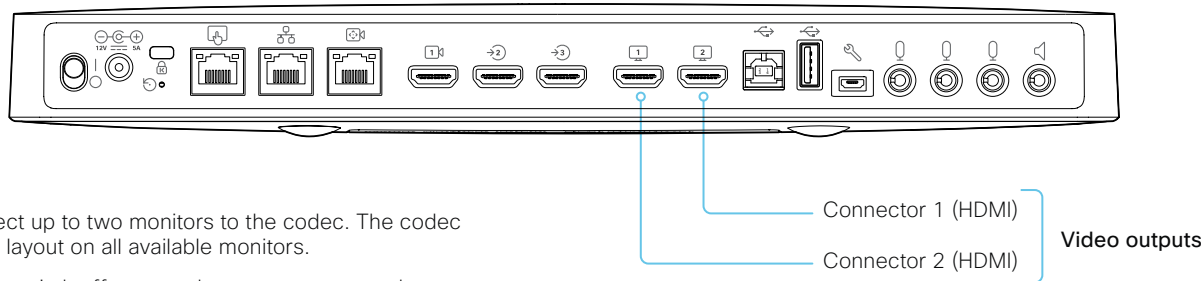
The device settings are grouped in categories. These are the same categories that you find in the web interface of the device. They also correspond to the API command path.

*Miscellaneous* is an exception to this rule. In this category you find settings that only can be set by CUCM. They don't correspond to a local setting on the device.


## Chapter 3

# Peripherals

## Connect monitors (page 1 of 2)



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

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

### Automatic setup

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

If the total number of monitors are two, the following settings will be assumed when set to **Auto**:

- [Video > Monitors: Dual](#)
- [Video > Output > Connector 1 > MonitorRole: First](#)
- [Video > Output > Connector 2 > MonitorRole: Second](#)

### When do you need manual setup

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

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

### About video outputs

Codec Plus has two HDMI outputs. These outputs can be used simultaneously.

Typically, the outputs are used for monitors or other displays.

The HDMI outputs support resolutions up to 3840 × 2160 at 60 fps. You need Premium HDMI cables to support the high resolutions and frame rates.

If the connected camera has loudspeakers (Quad Camera) there is no audio on the HDMI outputs. Otherwise there is audio on Connector 1.

## Connect monitors (page 2 of 2)

### Manual setup

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

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

#### Set a role for each monitor

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

Choose monitor roles that match your monitor setup.

#### Set the number of monitors

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

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

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

#### Choose on which monitor to display messages and indicators

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

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

#### Set the monitor resolution and refresh rate

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

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

### About the number of monitors and the role of each monitor

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

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

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

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

Note that a monitor can be reserved for presentations.

---

#### Example:

Two monitors in total, and the second monitor is dedicated to only show presentations:

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

## Connect input sources (page 1 of 2)

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

### About video inputs

Codec Plus has three HDMI inputs for cameras and computers. You can also connect other types of video and content sources.

HDMI video input 1 is reserved for the main camera.

### Connect a camera

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

Connect the additional cameras to Connector 2 (HDMI) and Connector 3 (HDMI).

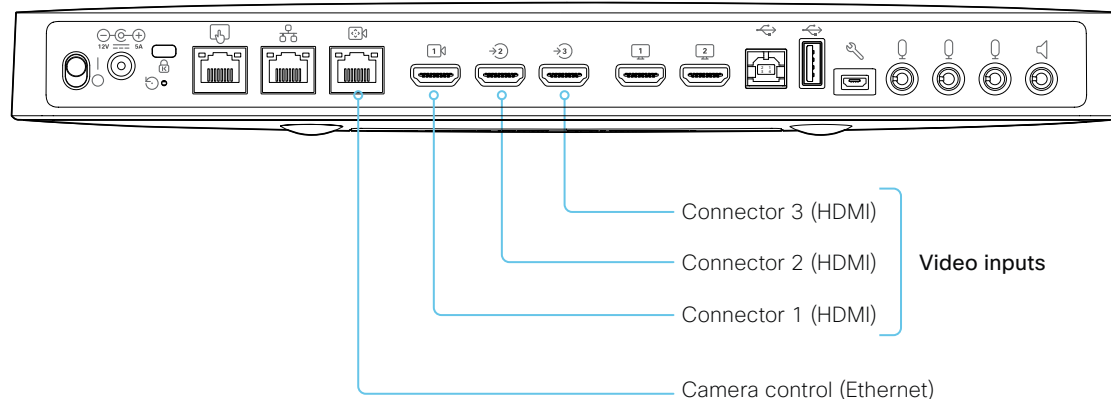
### Camera control

Camera control is through the Ethernet port. If you connect extra cameras you need an Ethernet switch to allow for camera control on all cameras.

### Connect a computer

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

Connect computers to Connector 2 (HDMI) or Connector 3 (HDMI)



### HDCP support

You can configure HDMI 2 (Input Connector 2) to support HDCP (High-bandwidth Digital Content Protection), which means that the device is authorized to display HDCP protected content.

- [Video > Input > Connector 2 > HDCP > Mode](#)

When this setting is **On**, the content from the source that is connected to HDMI 2 can only be played locally, you cannot share it with other conference participants while in a call. This applies whether the content is HDCP protected or not.

## Connect input sources (page 2 of 2)

### Set type and name for an input source

We recommend that you set type and name for an input source:

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

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

### About video and content quality

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

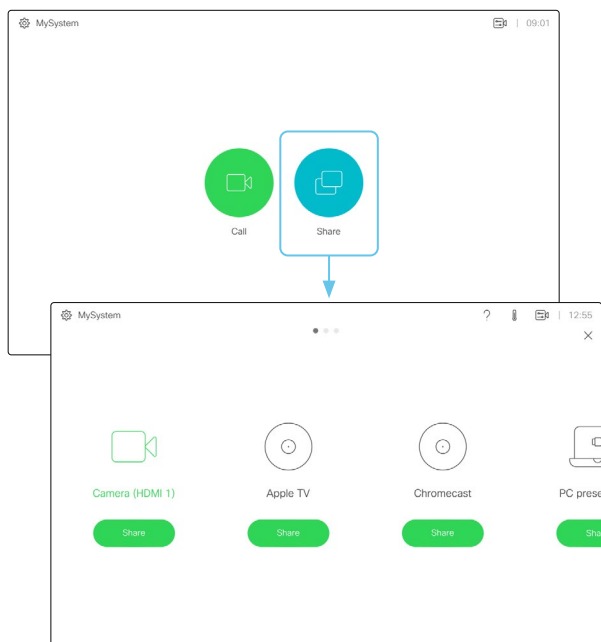
Typically, you should choose **Motion** when a large number of participants are present or when there is a lot of motion in the picture. Choose **Sharpness** when you want the highest quality of detailed images and graphics.

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

## 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 conferencing device.



User interface with multiple external input sources (example)

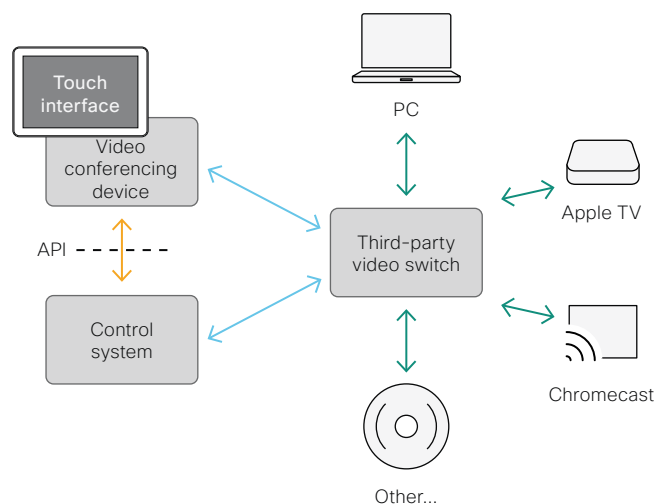
Consult the *Customization guide* for full details about how to extend the user interface, and how to use the device's API to set it up. Go to:

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

## Architecture

You need a Cisco video conferencing device 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 conferencing device, that controls the video switch.

When you program the control system you must use the video conferencing device'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, INTEGRATOR, or ADMIN user roles in order to access the API commands that you need when programming the control system.



## Information about displays

### Real-time communication requirements

We have put in a lot of effort to minimize the camera to screen delay on our video conferencing devices, 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

### Consumer Electronics Control (CEC)

The active video input on a display is sometimes changed by a user. The video input that is active is set from the manufacturer's user interface.

When you make a call the video conferencing device detects if the active video input on the display has been switched to another input. The video conferencing device then switches the input back so the video conferencing device is the active video input source.

If the video conferencing device goes into standby without being the active input source, the display will not be set to standby.

### Cisco recommended displays

Cisco recommends using the following displays for the best experience and verified compatibility. The list of displays is subject to change, check the CE9 Software Release Notes for updates.

Model	LG global website link
49" UHD (49UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C">http://www.lg.com/global/business/information-display/digital-signage/lg-49UH5C</a>
55" UHD (55UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C">http://www.lg.com/global/business/information-display/digital-signage/lg-55UH5C</a>
65" UHD (65UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C">http://www.lg.com/global/business/information-display/digital-signage/lg-65UH5C</a>
75" UHD (75UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C">http://www.lg.com/global/business/information-display/digital-signage/lg-75UH5C</a>
86" UHD (86UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C">http://www.lg.com/global/business/information-display/digital-signage/lg-86UH5C</a>
98" UHD (98UH5C)	<a href="http://www.lg.com/global/business/information-display/digital-signage/lg-98LS95D">http://www.lg.com/global/business/information-display/digital-signage/lg-98LS95D</a>

Model	Samsung global website link
QMN Series (43", 49", 55", 65", 75")	<a href="https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N">https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N</a>
QMH Series (49", 55", 65")	<a href="https://displaysolutions.samsung.com/digital-signage/detail/1144/QM49H">https://displaysolutions.samsung.com/digital-signage/detail/1144/QM49H</a>
QBN Series (43", 49", 55", 65", 75")	<a href="https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N">https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N</a>
QBH Series (65", 75")	<a href="https://displaysolutions.samsung.com/digital-signage/detail/1205/QB65H">https://displaysolutions.samsung.com/digital-signage/detail/1205/QB65H</a>

## Information about 4K resolution

### Connecting a display

When you start the device for the first time, the setup assistant starts automatically. This is where you test the display and adjust the settings. Follow the on-screen instructions.

If you need to adjust the settings at a later stage, sign in to the web interface, navigate to [Setup > Configuration > Video > Output > Connector n > Resolution](#), and adjust the screen resolution. Set the resolution according to what your display supports.

If your screen is black or flickering, you can set the resolution to a lower setting. If there still are problems, check that the HDMI cable is connected to an HDMI port on your display that supports Ultra HD. Check also that the HDMI Ultra HD settings are set to On on your display.

Cisco provides a list of displays that we have tested. Refer to the [Cisco recommended displays](#) chapter.

### Connecting a computer

If an error occurs when you connect a computer, a message will show on screen and on the Touch 10 controller.

The default preferred resolution on the video input connector is 1080p60 (1920\_1080\_60). If you want to use 4K resolution with the computer, sign in to the web interface, navigate to [Setup > Configuration > Video > Input > Connector n > PreferredResolution](#), and adjust the value.

Alternatively, you can override the resolution from the display/monitor configuration offered by the operating system of the connected computer.

### Checklist

For guaranteed operation, order HDMI cables from Cisco, or use certified HDMI cables. Refer to the [Information about HDMI cables](#) chapter.

Check that the video conferencing device's input/output connector(s) are configured correctly.

Check that the device (TV/display, computer) has support for 4K and that it is configured correctly.


The manufacturer may advertise that a TV/display supports 4K, but you should test the TV/display to make sure it works.

The need for high quality cables increases with 4K usage:

- 4kp30 uses about twice the data rate of 1080p60
- 4kp60 uses about four times the data rate of 1080p60

## Information about HDMI cables

HDMI cables are required for cameras, displays and presentation sources.

 For guaranteed operation we recommend that you order HDMI cables from Cisco\*, or use certified HDMI cables.

### HDMI cables for cameras and displays

The resolution formats larger than 1920×1200@60fps require use of high speed HDMI cables. For guaranteed operation, use HDMI cables that are pre-qualified from Cisco for use at 3840×2160@60fps, or use a cable that has passed the Premium HDMI Cable Certification Programme.

### HDMI cables for presentation sources

A presentation source can be a PC/laptop, document camera, media player, whiteboard, or other device.

The resolution formats larger than 1920×1080@60fps require use of high speed HDMI cables. For guaranteed operation, use a HDMI cable from Cisco, or use a cable that complies with the high speed HDMI 1.4b Category 2 specification.

We recommend that you order the HDMI presentation cable from Cisco (HDMI 1.4b Category 2).

You can find more information about HDMI cables at ► <http://www.hdmi.org>

\* The following products do not support Cisco's presentation cable for HDMI, Display Port, and Mini Display Port (CAB-HDMI-MULT-9M=): Room Kit, Room Kit Plus, Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, Room 70 G2, and Boards.

## Set up the SpeakerTrack feature

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

The speaker track feature uses automatic camera framing to select the best view based on how many people are in the room.

When closeup is enabled and a person in the room speaks, the device will find the person and select the best camera framing. The closeup may not include all the persons in the room. If you want all the persons in the room to be in the picture at all times you must turn off the closeup functionality.

### Best overview

The camera uses digital face detection to automatically create the best view of a single person or a group of people in the room. If people are moving around in the room or additional participants enters the room, the feature will adopt to the changes and automatically adjust the view to include all persons in the picture. This feature works together with speaker tracking to provide the best possible conferencing experience.

## Configure speaker tracking

Use the [Cameras > SpeakerTrack](#) settings to configure speaker tracking.

### [Cameras > SpeakerTrack > Mode](#)

**Auto:** Speaker tracking is enabled in general. The device will detect people in the room and automatically select the best camera framing. Users can switch speaker track on or off instantly in the camera control panel on the Touch controller.

**Off:** Speaker tracking is switched off, and it is not possible to switch it on from the user interface.

### [Cameras > SpeakerTrack > Closeup](#)

This setting only applies when the Cameras SpeakerTrack Mode is set to Auto.

**Auto:** The behavior depends on the device type. Boards will keep all the persons in the room in the camera framing at all times, while other devices will zoom in on the person speaking.

**Off:** The device will keep all the persons in the room in the camera framing at all times.

**On:** The device will zoom in on the person speaking.

## Products that support speaker tracking

The following Cisco products support speaker tracking:

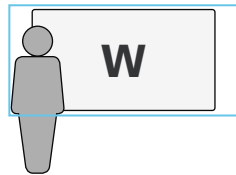
- MX700 and MX800 with dual camera
- SX80 with SpeakerTrack 60 camera or Quad camera
- Room Kit
- Codec Plus with Quad Camera (Room Kit Plus)
- Codec Pro with Quad Camera (Room Kit Pro) or SpeakerTrack 60 camera
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2
- Boards

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

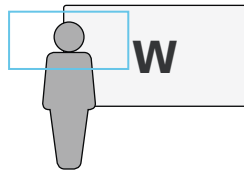
The Snap to Whiteboard feature extends the speaker tracking functionality, thus you need a camera that supports SpeakerTrack:

- MX700 and MX800 with dual camera
- SX80 with SpeakerTrack 60 camera or Quad camera
- Room Kit
- Codec Plus with Quad Camera (Room Kit Plus)
- Codec Pro with Quad Camera (Room Kit Pro) or SpeakerTrack 60 camera
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2

With the Snap to Whiteboard extension, the camera captures both the person and the whiteboard when a person next to the whiteboard is speaking.

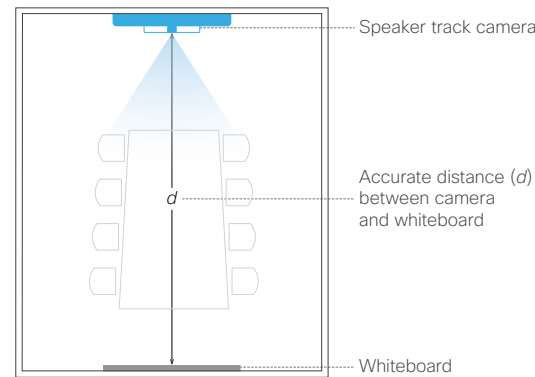


Without the Snap to Whiteboard extension, the camera captures only the person.



### Preparations

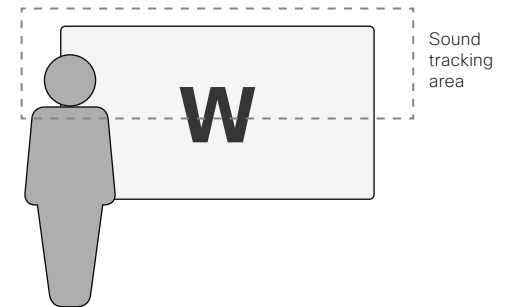
#### Whiteboard position



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

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

#### Speaker position



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

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

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

The Snap to Whiteboard wizard is only available when:

- [Cameras](#) > [SpeakerTrack](#) > [Mode](#) is **Auto**.



### Define the whiteboard area

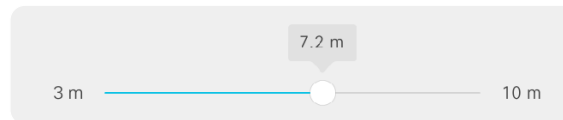
Use the wizard on the Touch controller to define the whiteboard area.

1. Tap the device name or address at the top of the user interface and open the [Settings](#) menu.
2. Tap [Snap to Whiteboard](#).

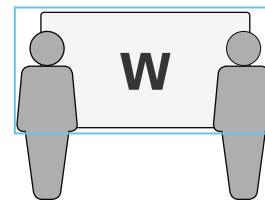
Sign in with ADMIN credentials if the [Settings](#) menu is passphrase protected on your device.



3. Tap [Configure](#) or [Reconfigure](#) to start the wizard (depends whether you configure the feature for the first time or not).

4. Follow the instructions in the wizard - use the back button  if you want to redo a step, and the next button  to move to the next step:
  - Move the slider to set the distance between the camera and the whiteboard. It is important that the distance is measured accurately.



- Adjust the camera view (pan, tilt, zoom) to frame the whiteboard. Leave some space on both sides for the person that will be speaking.



- Stand next to the whiteboard and start speaking.  
If the camera zooms to the view that you have chosen for the whiteboard, the feature is correctly set up, and ready to use. If not, see the troubleshooting notes to the right.
- Tap  to close the wizard, and  to close the Settings panel.

### Troubleshooting

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

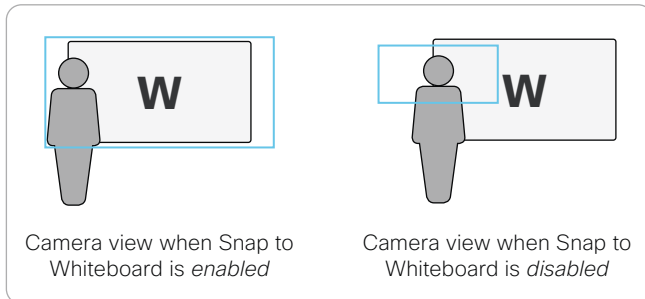
- Check that the whiteboard is placed across the room from the camera.
- Check that the distance between the camera and whiteboard is measured accurately.
- The person who is speaking must be close to the whiteboard. Furthermore, the person must stand upright so that the sound comes from the upper half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

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

### Enable and disable Snap to Whiteboard

You can enable or disable the Snap to Whiteboard feature from the *Settings* menu on the Touch controller or from the web interface.

**i** If the Settings menu on the Touch controller is open (not protected by the ADMIN passphrase), any user can switch the feature On and Off during a meeting or between meetings. Moreover, any user can reconfigure the feature.



#### From the Touch controller

1. Tap the device name or address at the top of the user interface and open the *Settings* menu.
2. Tap *Snap to Whiteboard*.

Sign in with ADMIN credentials if the *Settings* menu is protected by a passphrase on your device.

3. Set the toggle switch to:

**Enabled:** Snap to Whiteboard is enabled, and the camera will capture both the person that speaks and the whiteboard he or she is standing next to.

**Disabled:** Snap to Whiteboard is disabled, and the camera will capture only the person that speaks.

#### From the web interface

1. Sign in to the web interface and navigate to *Setup > Configuration*.
2. Find the *Cameras > SpeakerTrack > Whiteboard > Mode* setting.

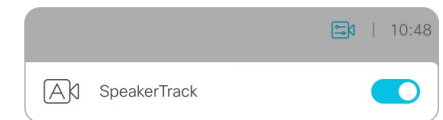
**On:** Snap to Whiteboard is enabled, and the camera will capture both the person that speaks and the whiteboard he or she is standing next to.

**Off:** Snap to Whiteboard is disabled, and the camera will capture only the person that speaks.

### How to switch on speaker tracking

Speaker tracking, which can be switched on and off by the user at any time, must be switched on for the Snap to Whiteboard extension to work.

Tap the camera icon in the status bar of the Touch controller, and use the toggle button to switch speaker tracking on and off.



## Set up the PresenterTrack feature (page 1 of 4)

The PresenterTrack feature enables the camera to follow a presenter that is moving about on stage. The tracking stops when the presenter leaves the stage.

The following cameras and video conferencing devices support PresenterTrack:

- Codec Plus with Precision 60 camera
- Codec Pro with Precision 60 or SpeakerTrack 60 camera
- SX80 with Precision 60 or SpeakerTrack 60 camera
- Room 55 Dual with Precision 60 as external camera
- Room 70 with Precision 60 as external camera
- Room 70 G2 with Precision 60 as external camera
- MX700 or MX800 with single or dual camera

### Capabilities and limitations

- Once set up, the user can activate and deactivate PresenterTrack from the camera panel on the Touch controller.
- The camera uses digital pan, tilt, and zoom, so it doesn't move physically while tracking the presenter.
- PresenterTrack supports the tracking of one or more persons on stage. If they stand too far apart to fit within a zoomed view, the camera zooms out to show the full stage.
- You can use PresenterTrack as a standalone feature, or as part of the Briefing Room and Classroom scenarios.
- You can set up the device to use one of the cameras in a SpeakerTrack 60 camera assembly (or in an MX700/MX800 dual camera) for PresenterTrack.
- You cannot use PresenterTrack and SpeakerTrack simultaneously. When you activate PresenterTrack, SpeakerTrack is disabled automatically. And also the other way around, when you activate PresenterTrack, SpeakerTrack is disabled automatically.

There is one exception to this: In the Briefing Room and Classroom scenarios both features are active simultaneously in the Q&A mode (when someone in the local audience asks a question, while the device is in *Local Presenter* mode).

### Considerations before placing the camera

When you set up PresenterTrack, you must define a stage area and a trigger zone. Consider the location and use of these areas when placing the camera that is tracking the presenter on stage.

We recommend you to be in the same room as the video conferencing device and camera while setting up PresenterTrack.

#### Stage area

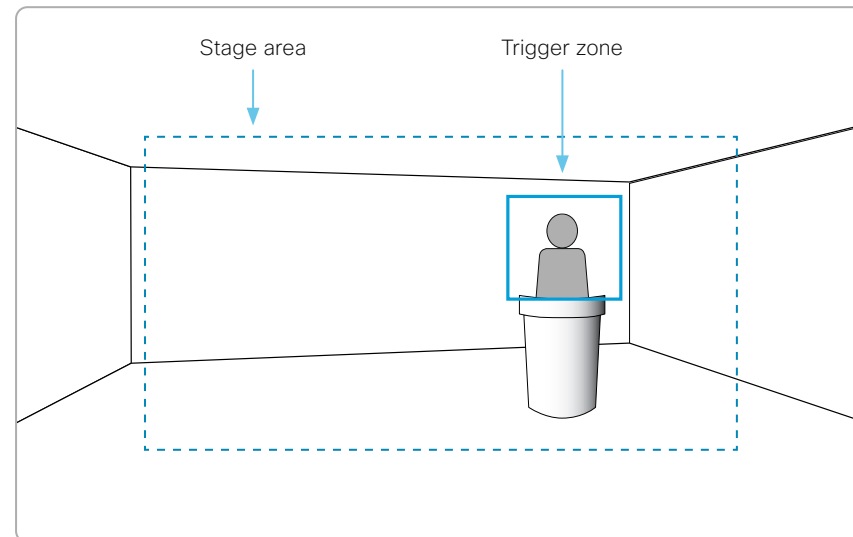
The stage area is the zoomed-out overview image.

- Make it large enough so that the presenter can move about on stage. The tracking stops when the presenter leaves the stage area.
- Allow the audience or meeting participants to move naturally in the room without triggering the tracking.

#### Trigger zone

Presenter tracking doesn't start before the camera detects a face in the trigger zone.

- Choose a location where the presenter naturally enters the stage, for example by a presenter table or podium.
- Make it large enough for the camera to detect the face of the presenter.
- To avoid a false face detection, make sure that the background of the trigger zone is neutral. Avoid having the trigger zone in front of a screen.






## Set up the PresenterTrack feature (page 2 of 4)

### Set up and test PresenterTrack

We recommend you to be in the same room as the video conferencing device and camera while setting up PresenterTrack.

1. Sign in to the web interface and navigate to [Setup > Presenter Tracking](#).
2. Check [Enable PresenterTrack](#) and click [Configure...](#) to open the configuration page.

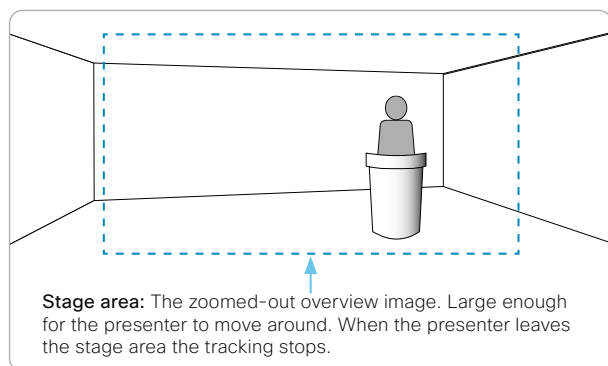
Opening this page deactivates standby and presenter tracking, enables the self-view in full screen, and shows the trigger zone rectangle on the screen of the device.

 Don't leave this web page without clicking [Done](#), otherwise the trigger zone rectangle stays visible on the screen of the device.

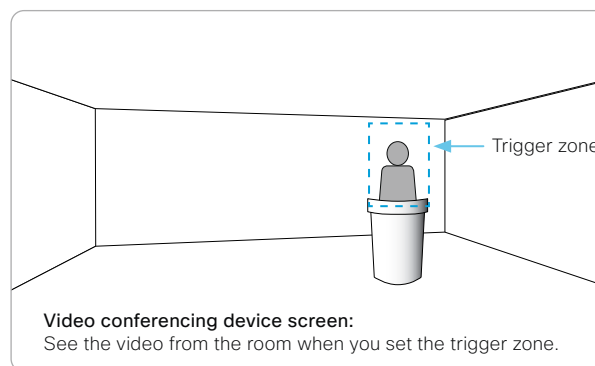
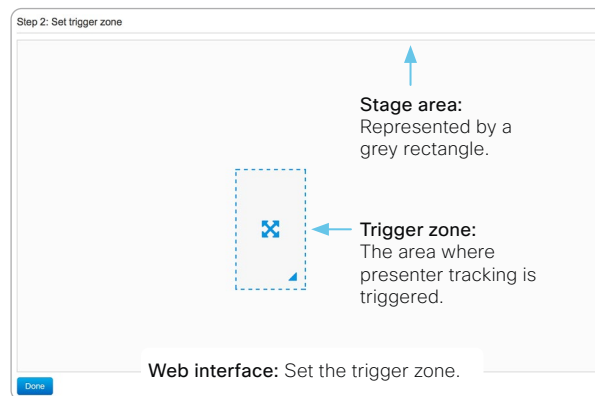
Alternatively, you can remove the rectangle by tapping the [Camera icon](#) on the Touch controller and choose a camera position from the list.

3. Choose a camera from the [Camera source](#) drop down list and use the camera controls (zoom, pan, tilt) on the Touch controller to define the stage area.

You see a notification if the camera does not support the PresenterTrack feature.



4. A blue dashed rectangle, which represents the trigger zone, is shown on the web interface. Move and resize the rectangle while watching the screen of the device. You see the same rectangle overlaying the camera self-view. Place the rectangle where you want the trigger zone to be.



If you want to set up a more advanced polygonal trigger zone, see the sidebar.

5. Click [Done](#).

### Set up a polygonal trigger zone

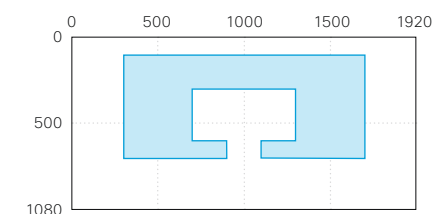
You can set up only rectangular trigger zones from the [Presenter Tracking](#) web page.

If you want to define a more advanced polygonal trigger zone, you must go to the [Setup > Configuration](#) page, and find the [Cameras > PresenterTrack > TriggerZone](#) setting.

The value of this setting is a string that contains the coordinate pairs of all the vertices of the polygon.

#### Example:

Define the following trigger zone, which has 12 vertices. Such a trigger zone may be convenient if there is a screen, which you want to avoid, behind the presenter.



The coordinates of the vertices are:

(300,100)	(1100,600)	(700,600)
(1700,100)	(1300,600)	(900,600)
(1700,700)	(1300,300)	(900,700)
(1100,700)	(700,300)	(300,700)

The corresponding setting value is:

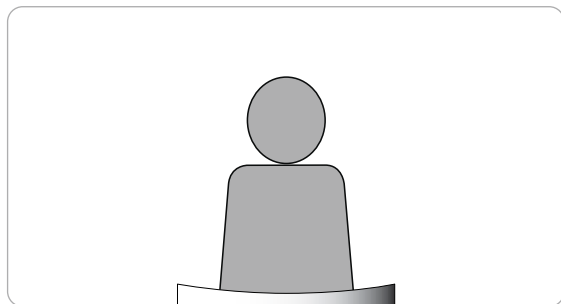
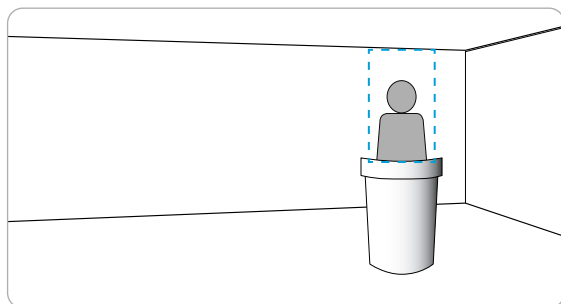
[Cameras > PresenterTrack > TriggerZone:](#)  
 300,100,1700,100,1700,700,1100,700,  
 1100,600,1300,600,1300,300,700,300,  
 700,600,900,600,900,700,300,700

## Set up the PresenterTrack feature (page 3 of 4)

6. Tap the *Camera* icon in the upper right corner of the Touch controller and choose *Presenter* from the list of camera positions.

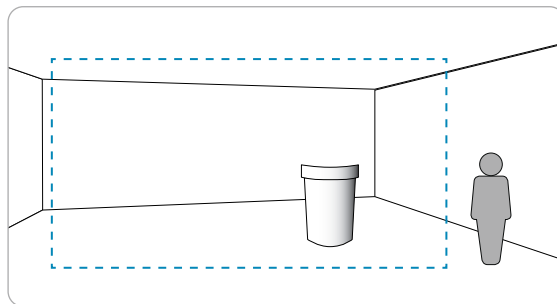
This activates presenter tracking.

7. Position yourself in the trigger zone and see that the camera zooms in on you.



8. Walk about on the stage and check that the camera follows you.

9. Check that presenter tracking stops when you leave the stage.



If something fails, go back to step 3, 4 and 5 to adjust the size and location of the stage area and the trigger zone.

For more troubleshooting help, you can switch on PresenterTrack *Diagnostics Mode*, as described on the next page.

### Temporarily activate or deactivate PresenterTrack

During a meeting, you can use the Touch controller to temporarily activate or deactivate presenter tracking.

1. Tap the *Camera* icon in the status bar.
2. Select *Presenter* in the list of camera positions to activate presenter tracking.

Deselect *Presenter* in the list of camera positions to deactivate presenter tracking.

If presenter tracking has been deactivated, the presenter must enter the trigger zone again in order for tracking to start.

## Set up the PresenterTrack feature (page 4 of 4)

### Diagnostics mode

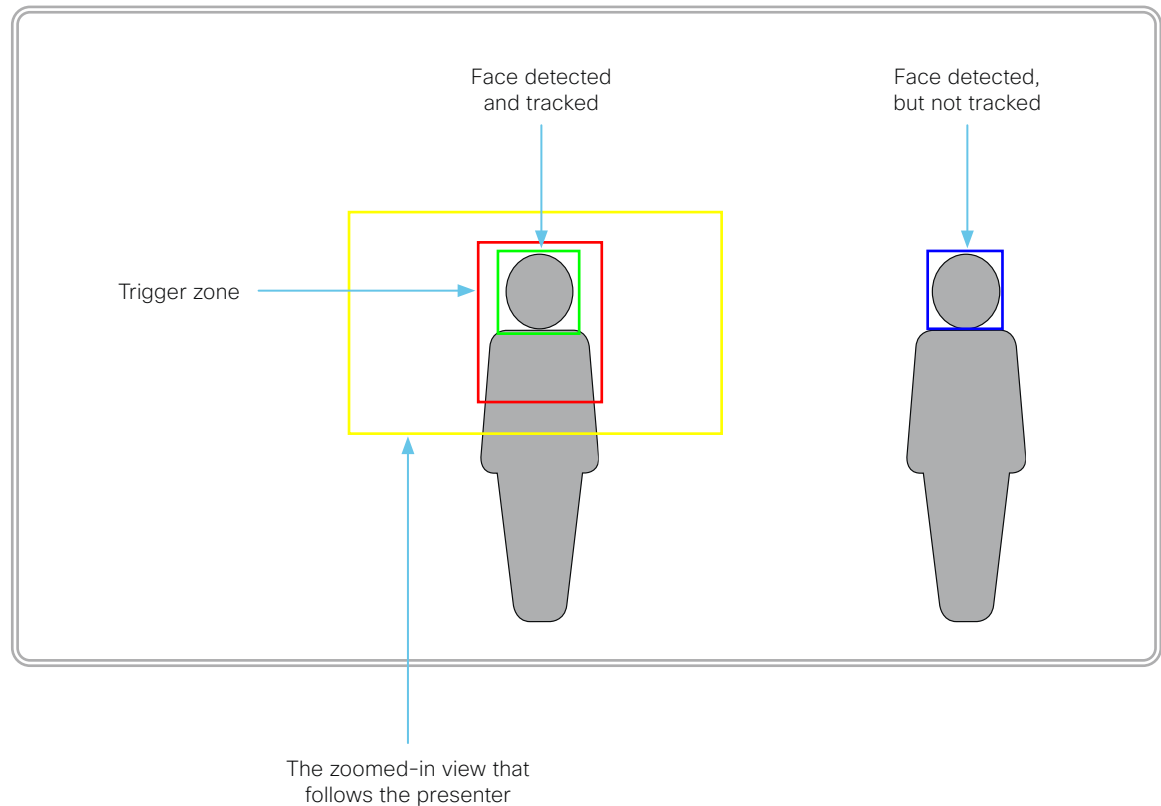
The PresenterTrack diagnostics mode may be a helpful tool when troubleshooting an issue. In order to set the device in diagnostics mode, you have to use the xAPI of the device.

Sign in to the xAPI and run the following command:

- `xCommand Cameras PresenterTrack Set Mode: Diagnostic`

In this mode, you see the stage area (the zoomed-out overview image) on the screen, and an overlay with the following indicators::

- RED frame: The trigger zone.
- YELLOW frame: The zoomed-in view of the presenter.
- GREEN frame: A face that is detected and tracked.
- GREEN or RED blinking filled frame: Face detections. Green color indicates a high confidence, red color indicates a low confidence.
- BLUE: A face is detected but the face is not tracked.



## Classroom set-up (page 1 of 5)

The *Classroom* set-up makes it easy to set up, manage, and use a room to deliver training and education sessions to groups of people.

The *Classroom* set-up is available as a room type template. When you set up a room using a template, a set of configurations is pushed automatically to the device. It is important that the room is set up correctly, and that the cameras are connected exactly as specified. Otherwise the configurations will not match the room.

### Required equipment

- One of the following devices:
  - SX80, Codec Pro, Codec Plus
  - MX700, MX800
  - Room 55 Dual
  - Room 70
  - Room 70 G2
- One or more screens (configurable)
- Two cameras (Audience camera and Presenter camera)
- Microphones
- Speakers
- Touch 10 controller

### Limitations

Not supported functionality when using Classroom:

- MultiSite (embedded multipoint switch)
- Content sharing to Proximity clients
- Directional audio
- Snap to Whiteboard

### Room modes

The *Classroom* set-up has the following predefined room modes that accommodate different scenarios: Local Presenter, Remote Presenter, and Discussion.

#### Local Presenter mode

- The presenter is in the room. This mode also covers the case when someone in the local audience asks a question (Q&A).
- If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* detects a presenter in the room.
- Sends video from the *Presenter camera* to the far end. In the Q&A case: Sends split-screen video from the *Presenter camera* and the person asking the question (*Audience camera*) to the far end.

#### Remote Presenter mode

- The presenter is calling in.
- If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* doesn't detect a presenter in the room.
- Sends video from the *Audience camera* to the far end.

#### Discussion mode

- For discussions between different sites. A local presenter is in the room.
- Always use the Touch 10 controller to activate this mode.
- Sends video from the *Audience camera* to the far end.

### Classroom versus Briefing Room set-up

The *Classroom* set-up is more flexible than the *Briefing room* set-up in the number of screens and how the layout is distributed on the screens. Also, more products support *Classroom*.

#### Classroom

- Supported products: Codec Plus, Codec Pro, SX80, Room 55 Dual, Room 70, Room 70 G2, MX700, and MX800
- You can use any number of screens that the device supports, typically two or three. Use the video monitor settings to configure the distribution of layouts on the screens, if the default behavior does not fulfill your requirements.

#### Briefing room

- Supported products: Codec Pro, SX80, Room 70 G2, MX700, and MX800
- The set-up requires three screens, and the layouts on the screens are preconfigured (and fixed) to match that particular scenario.

## Classroom set-up (page 2 of 5)

### Room arrangement examples

These illustrations show examples of how to arrange screens, cameras and microphones, and where to place people for the best experience.

#### Recommendation

##### Audience camera:

- Use the integrated camera for video conferencing devices that have that. For other devices, we recommend the Cisco Quad Camera or Cisco TelePresence SpeakerTrack 60 camera. We recommend a camera with speaker tracking, but it is also possible to use a camera without speaker tracking capabilities.

##### Presenter camera:

- Cisco TelePresence Precision 60 with presenter tracking enabled.

##### Microphones:

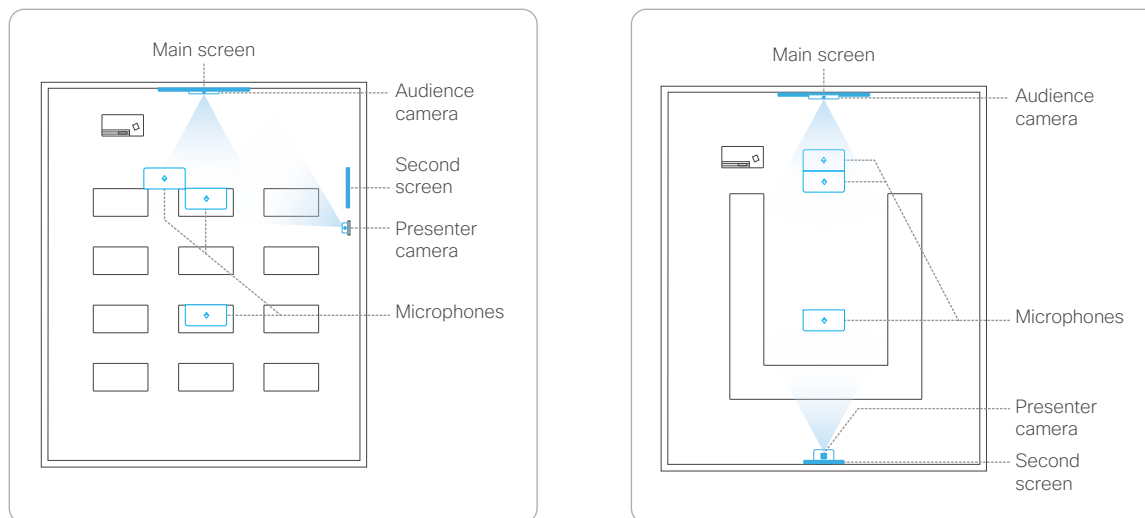
- We recommend the Cisco TelePresence Ceiling Microphone for good coverage of the room. Also other microphone solutions can be used.

##### Speakers:

- Use the integrated speakers for video conferencing devices that have that. For other devices, we recommend good quality stereo speakers placed next to the main screen at the front of the room.


##### Screens:

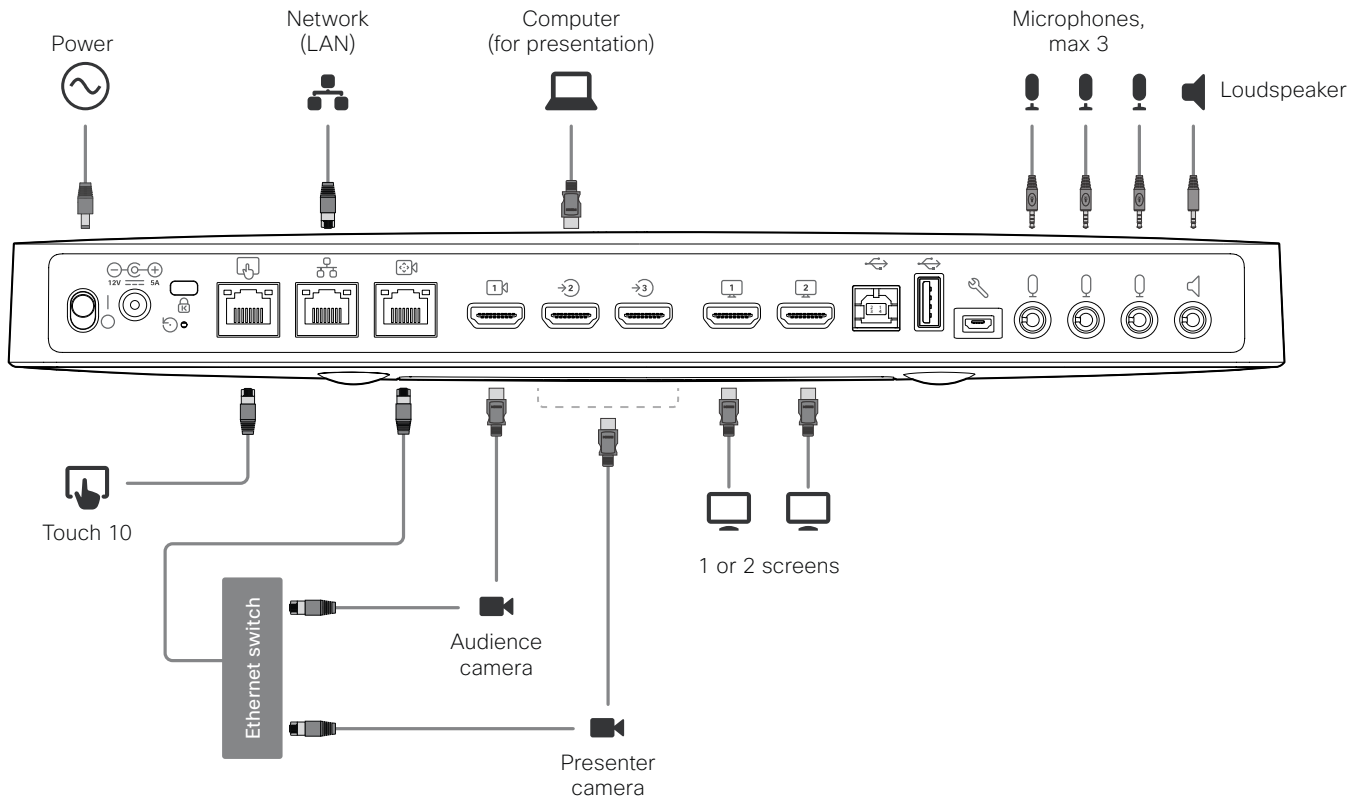
- You can use one or more screens (the maximum number of screens depends on your type of device).
- For most set-ups, we recommend that you use two screens or more. Place the main screen at the front of the room. Place a second screen on the side or at the back, so that the local presenter can see the remote audience.



## Classroom set-up (page 3 of 5)

### Connect cables

 Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Classroom* room type template, match your actual set-up.



## Classroom set-up (page 4 of 5)

### Configure the device

We recommend you to be in the same room when setting up the Classroom. Otherwise you are not able to set up PresenterTrack properly.

1. Connect cameras and screens as described on the previous page.
2. Use the Touch controller to stop sharing the video from the *Presenter camera*. It is important that video from the *Presenter camera* is not displayed on any screen while setting up Classroom.
3. Sign in to the web interface and navigate to [Setup > Configuration](#).
4. Go to the [Video > Input > Connector n](#) section, and set the following (note that *n* is the number of the Connector where the *Presenter Camera* is connected):
  - [InputSourceType](#): **camera**
  - [PresentationSelection](#): **Manual**
  - [Quality](#): **Motion**
  - [Visibility](#): **Never**
  - [CameraControl Mode](#): **On**

Click [Save](#) for the changes to take effect.
5. Set up PresenterTrack for the *Presenter camera*, see the [▶ Set up the PresenterTrack feature](#) chapter.
 

This feature enables the camera to follow a presenter that is moving about on stage.
6. Navigate to [Setup > Configuration](#). Go to the [Cameras > PresenterTrack > PresenterDetectedStatus](#) and choose whether to enable (default) or disable automatic switching between *Local Presenter* and *Remote Presenter* modes.
 

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

Read more about switching between modes on the next page.
7. If the default screen and layout behavior does not suit your set-up, you must configure the screens and layouts using the following settings:
  - [Video > Monitors](#): Defines the number of different layouts in your room set-up.
  - [Video > Output > Connector n > MonitorRole](#): Defines which layout each screen gets. Screens with different monitor roles get different layouts.

Refer to the chapter about connecting monitors for details.
8. Navigate to [Setup > Room Types](#), and click the [Classroom](#) thumbnail to push the corresponding configuration to the device.

## Classroom set-up (page 5 of 5)

### Switching between room modes

Switching between room modes (*Local Presenter*, *Remote Presenter*, *Discussions*), which implies that camera input sources, and remote and local screen layouts, are changed, can be done in two ways:

- Automatically, based on who is speaking and whether a local presenter is present on stage.

Automatic switching is only between the *Local Presenter* and *Remote Presenter* modes. The room mode doesn't change automatically if the current mode is *Discussion*.

Automatic switching is supported only when the PresenterTrack feature enabled (*Cameras > PresenterTrack > Enabled* set to **True**).

- Manually, using the buttons on the Touch controller.

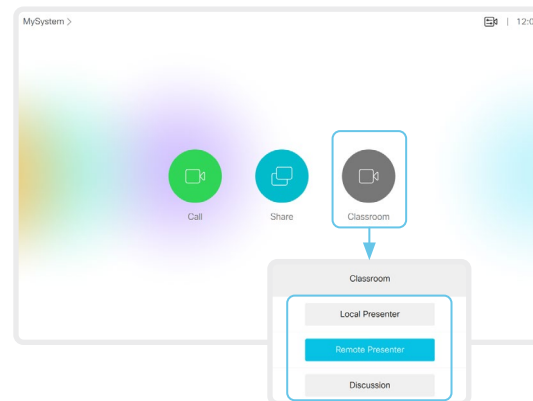
Automatic switching implies:

- The device switches to the *Local Presenter* mode when a person is detected in the PresenterTrack trigger zone.
- The device switches to the *Remote Presenter* mode when the local presenter, who is tracked, leaves the stage.
- If someone in the local audience asks a question when the device is in *Local Presenter* mode, the device sends split-screen video showing both the presenter and the person asking the question. This behavior requires a SpeakerTrack 60 or Quad Camera as *Audience camera*, and that speaker tracking is switched on.

### Switch between room modes manually

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

- Tap *Classroom* on the Touch controller.
- Tap the mode you want to change to: *Local Presenter*, *Remote Presenter*, or *Discussion*. The current mode is highlighted.





## Connect the Touch 10 controller (page 1 of 4)

Touch 10 must either be directly connected to the video conferencing device as described on this page, or paired to the device via the network (LAN) as described on the next page. The latter is referred to as remote pairing.

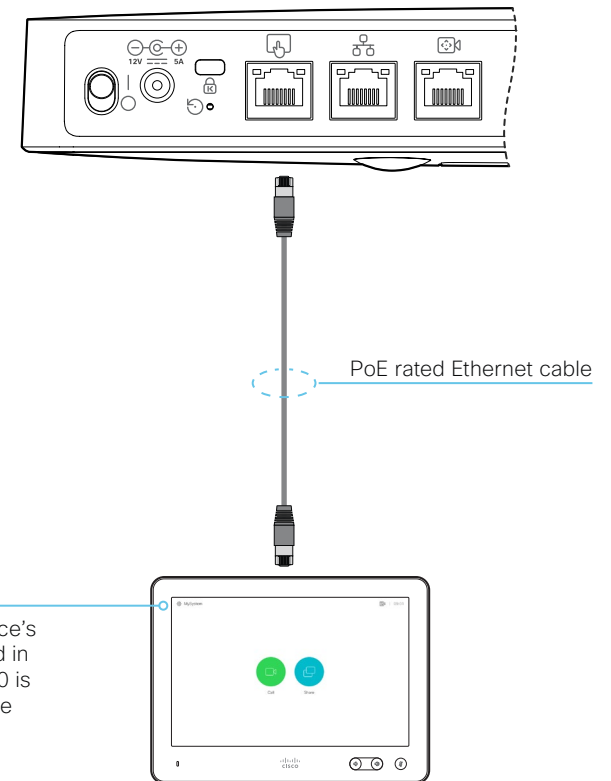
### Connect Touch 10 directly to the video conferencing device

Connect Touch 10 to the video conferencing device's dedicated Touch (RJ-45) port as illustrated.

#### Touch 10 set-up

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

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



#### Contact information

The video conferencing device's name or address is displayed in the status bar when Touch 10 is successfully connected to the device.

The Ethernet connector is at the rear of Touch 10.

## Connect the Touch 10 controller (page 2 of 4)

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

Connect Touch 10 and the video conferencing device 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 devices signalling that they are available for pairing will show up on the screen. Tap the name of the device you want to pair with.

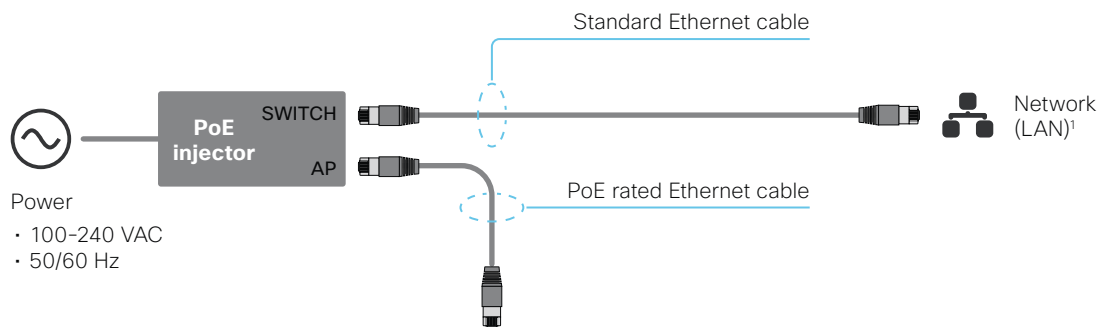
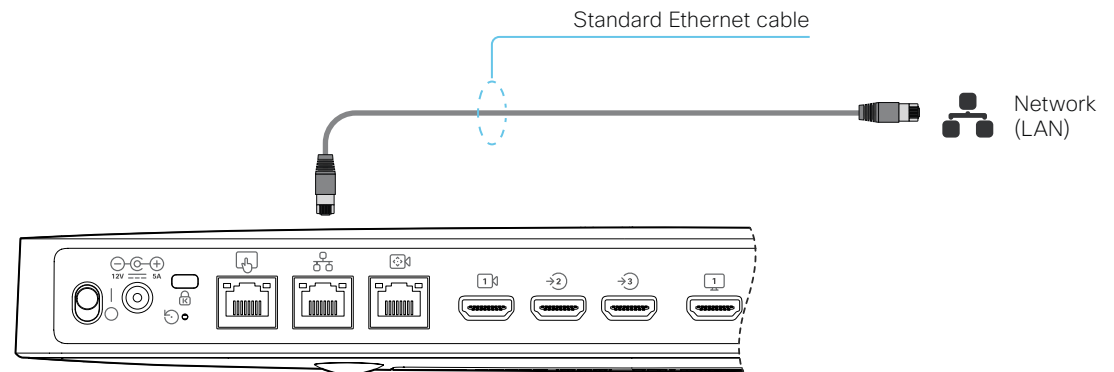
Note that the following must be fulfilled for a device to show up in the list:

- The device and Touch 10 must be on the same subnet.
- The device must have been restarted within the last 10 minutes. If the device does not appear in the list, try restarting it.
- If the device does not appear in the list of available devices, enter its IP address or hostname in the input field. Tap *Connect*.
- You have to log in with username and passphrase for the pairing process to commence. Tap *Login*.

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

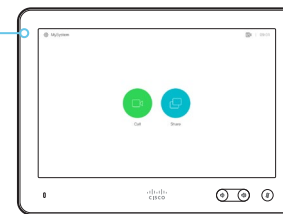
Read more about how to create a user account and assign a role to it in the [User administration](#) chapter.

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



#### Contact information

The video conferencing device's name or address is displayed in the status bar when Touch 10 is successfully paired to the device.



The Ethernet connector is at the rear of Touch 10.

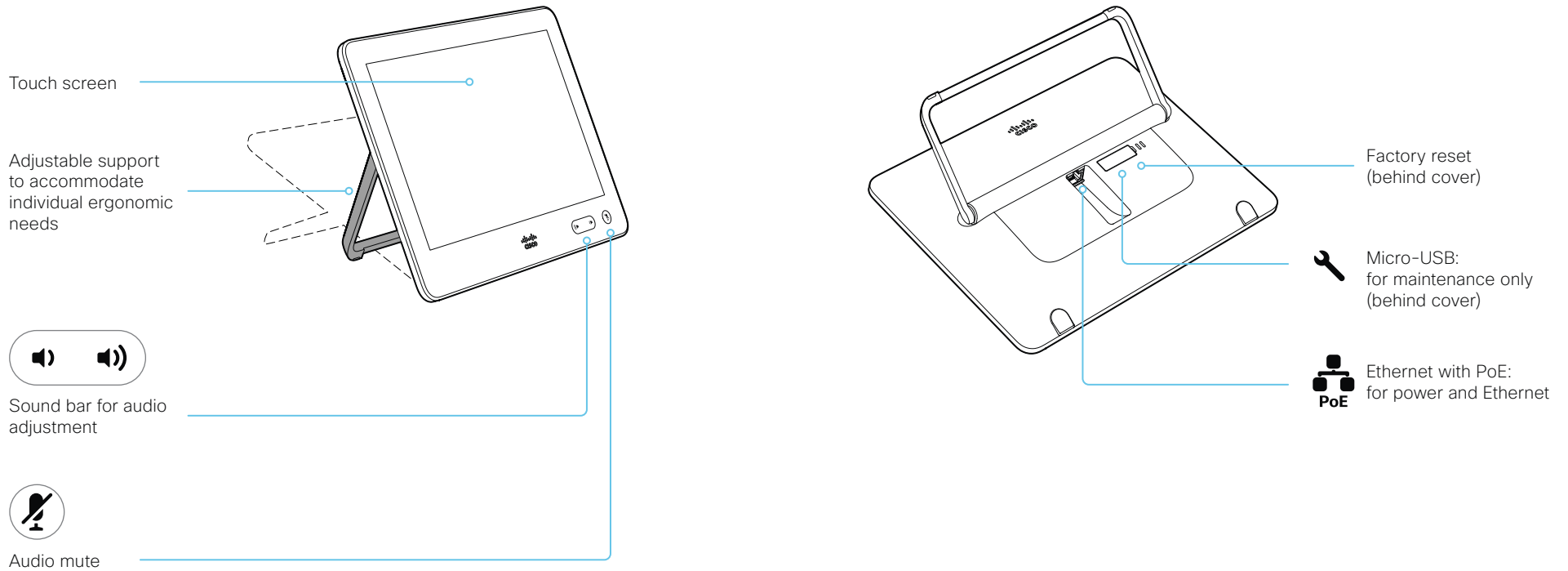
<sup>1</sup> If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

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).

## Connect the Touch 10 controller (page 3 of 4)

### Cisco Touch 10 physical interface

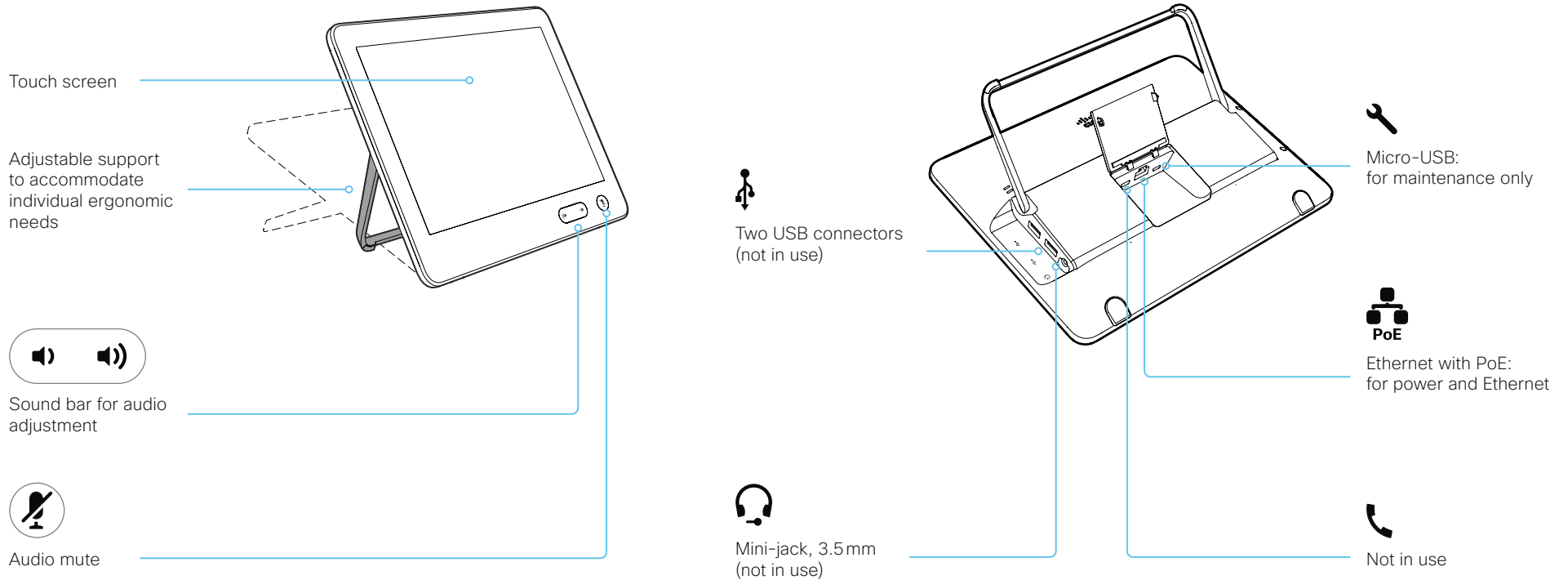
This is the new version of the Touch 10 controller launched late 2017. It has the same functionality as the previous version, but has a slightly different physical interface. The new device is identified by the logo on front, and fewer connectors at the back.



## Connect the Touch 10 controller (page 4 of 4)

### Cisco TelePresence Touch 10 physical interface

See next page for a newer version of the Touch 10 controller.



## Connect the ISDN Link

The ISDN Link enables a video conferencing device to use ISDN lines for connectivity, and enables both video calls and telephone calls over the PSTN (Public Switched Telephone Network).

ISDN Link support ISDN BRI, ISDN PRI and V.35. ISDN can be used in addition to regular IP connectivity for SIP or H.323 calls, or without any IP infrastructure.

ISDN Link is managed from the video conferencing device's web interface. Sign in to the web interface and navigate to [Setup > Peripherals](#).

Requirements and limitations:

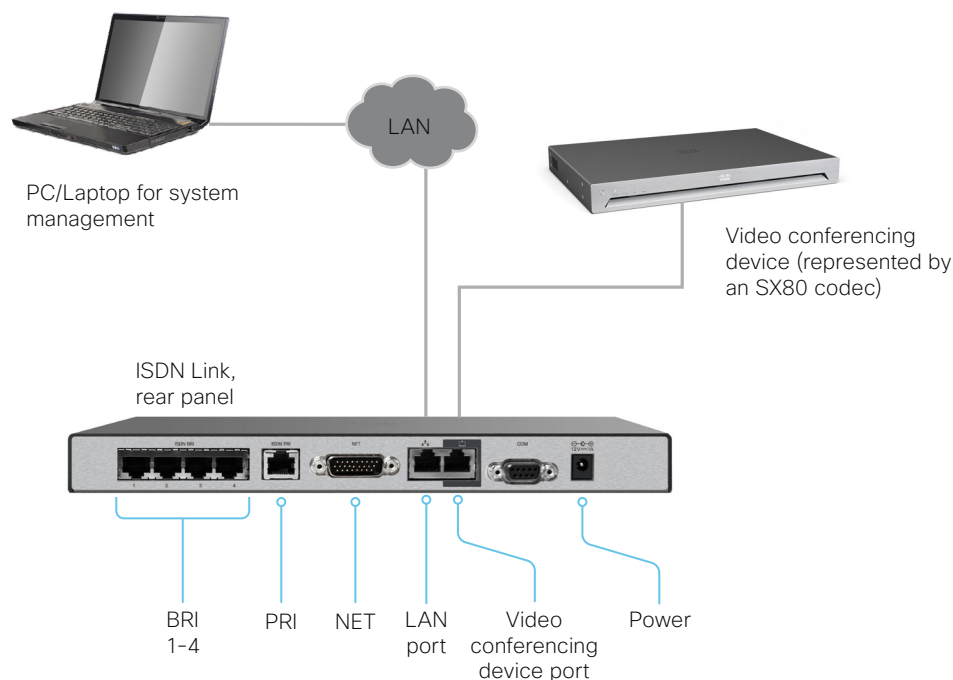
- The ISDN Link must be running IL1.1.7 software or later
- The video conferencing device must be running CE9.3 software or later. The video conferencing device must have IPv6 enabled in the web interface or API in order to communicate with the ISDN Link
- Observe the network topology in the ISDN Link Installation Guide in order to guarantee a successful installation
- The video conferencing device and ISDN Link must be on the same subnet. If the endpoint or ISDN Link are assigned new IP addresses they will only remain paired as long as they are kept in the same subnet.
- Video conferencing devices that are registered to the Cisco Webex cloud service are not able to use ISDN Link.

### Setup and configuration

More information about ISDN Link (Release Notes, Installation Guide, Administrator Guide, API Guide, Compliance and Safety guide) is found here: <https://www.cisco.com/go/isdnlink-docs>

Setup with LAN and direct connection between the video conferencing device and ISDN Link

This is the recommended setup. But there are other options, so see the user documentation for additional examples: <https://www.cisco.com/go/isdnlink-docs>



## Chapter 4

# Maintenance

## Upgrade the device software

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

### Download new software

Each software version has a unique file name. Go to the Cisco Download Software web page, and select your product:

► <https://software.cisco.com/download/home>

The format of the file name is:

"cmterm-s53200ce9\_10\_x-yyy.k3.cop.sgn"

where "x" represents the dot dot release number, and "yyy" represents a unique identifier of the software.

### Install new software

Download the appropriate software package and store it on your computer. This is a .cop.sgn file. Don't change the file name.

1. Click [Browse...](#) and find the .cop.sgn 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 device restarts automatically after the installation.

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

### Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (CE9).

Go to: ► <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/tsd-products-support-series-home.html>

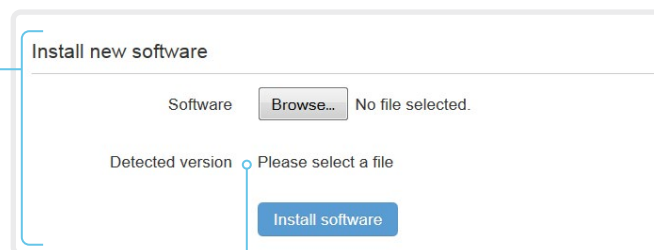
### Software download

Go to the Cisco Download Software web page, and select your product: ► <https://software.cisco.com/download/home>

Use COP files when upgrading Boards and Room series devices from the web interface or TMS.

The SX, MX and DX series also support PKG files.

CUCM uses COP files for all products.



### Check new software version

When you have selected a file, the software version is shown here

## 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 device.

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

### The device's serial number

You need the device'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 device 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 device.

Each device 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.



## Device status

### Device information overview

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

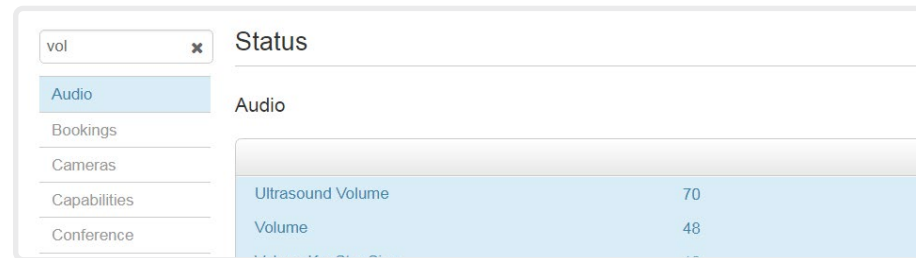
This page shows the product type, device name and basic information about the hardware, software, installed options and network address. Registration status for the video networks (SIP and H.323) is included, as well as the number/URI to use when making a call to the device.

### Detailed device 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

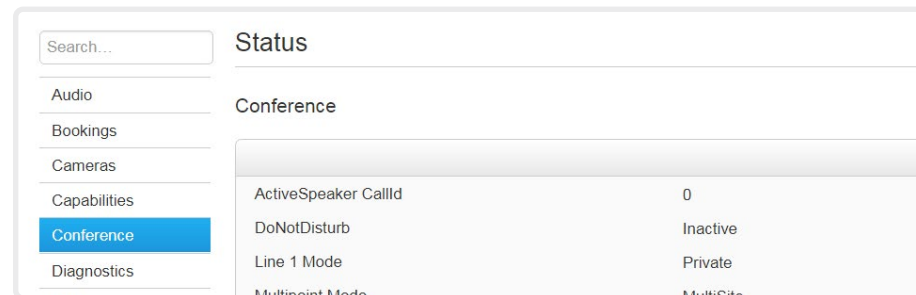
Enter as many letters as needed in the search field. All entries that contain these letters are shown in the right pane. Entries that have these letters in their value space are also shown.



Status	
Audio	
Ultrasound Volume	70
Volume	48

### Select a category and navigate to the correct status

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



Status	
Conference	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private

\* The status shown in the illustration serve as an example. The status of your device 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 [Wake up the system](#) to wake up a device that is in standby mode.

**Diagnostics** Wake up the system Re-run diagnostics

Diagnostics help identify issues that may cause the system to fail or not work as expected.

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

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

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

**OK:** Standby Control  
The system goes into standby automatically after 10 minutes. Standby can be configured through the [system configuration](#).

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

## Download log files

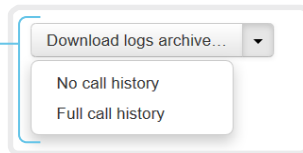
Sign in to the web interface and navigate to [Maintenance > System Logs](#).

### 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.

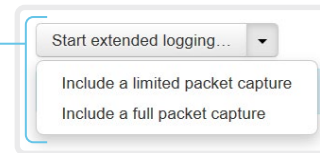
### Start extended logging

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.



### Refresh a log file list

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



## About log files

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

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

All current log files are archived in a time stamped *historical log file* each time the device 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 device's resources, and may cause the device to under-perform. Only use extended logging mode when you are troubleshooting an issue.

## Create a remote support user

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

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

### Create remote support user

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

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

The system does not have an active Remote Support User.

[Create user](#) [Delete user](#)

**This user is valid until**  
2018-10-05 16:50:18

**Token**

```
bgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5z1+b
TQek1PaSpsQJNEMfzThgbvK4J7pgOyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
e9CpAoRNq+mZMqEG1lsswKPZ7HYulvyVTH/XuPzU7Nues
9pwzLc8BFgBt1xV0fKeoeOmMX+it1Ecamln4lnXlScgOt
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 device you can create a remote support user.

The remote support user is granted read access to the device 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 and restore configurations and custom elements

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

You can include custom elements as well as configurations in a backup file (zip-format). You can choose which of the following elements to include in the bundle:

- Branding images
- Macros
- Favorites
- Sign-in banner
- UI extensions
- Configurations/settings (all or a sub-set)

The backup file can either be restored manually from the device's web interface, or you can generalize the backup bundle so that it can be provisioned across multiple devices, for example using Cisco UCM or TMS (see the **next** chapters).

### Create a backup file

1. Open the [Create backup](#) tab.
2. Select the elements you want to include in the backup file.  
Elements that currently don't exist on the device are greyed out.
3. Select which settings - if any - you want to include in the backup file. Note the following:
  - As default, all settings are included in the backup file.
  - You can remove one or more settings manually by deleting them from the list on the web page.
  - If you want to remove all settings that are specific to one device, click [Remove system-specific configurations](#).  
This is useful if you are going to restore the backup bundle on other devices.
4. Click [Download backup](#) to store the elements in a zip-file on your computer.

### Restore a backup file

1. Choose the [Restore backup](#) tab.
2. Click [Browse...](#) and find the backup file you want to restore.  
All settings and elements in the backup file will be applied.
3. Click [Upload file](#) to apply the backup.  
Some settings may require that you restart the device before they take effect.

### Additional information

#### Restoring macros

If a backup file that contains macros is restored on a device the following applies:

- The macro runtime is started or restarted.
- The macros are automatically activated (started).

#### Restoring branding images

If a backup bundle contains branding images, the *UserInterface Wallpaper* setting is automatically set to **Auto**.

This means that the branding images will automatically be displayed, possibly replacing a custom wallpaper.

#### The backup file

The backup file is a zip-file that contains several files. It is important that the files are at the top level within the zip-file, and not include in a folder.


## CUCM provisioning of custom elements

A backup file, as described in the ► [Backup and restore configurations and custom elements](#) chapter, can be used as a *customization template* for multiple devices.

The customization template (backup file) may be hosted on either:

- the CUCM TFTP file service, or
- a custom web server that can be reached by the devices on HTTP or HTTPS.

When a device get information from CUCM (Cisco Unified Communications Manager) about the name and location of a customization template, the device will contact the server, download the file, and restore the custom elements.

 Configurations will not be restored on the device, even if they are part of the backup file that you use as a customization template.

Upload a customization template to the TFTP file server

1. Sign in to *Cisco Unified OS Administration*.
2. Navigate to *Software Upgrades > TFTP File Management*.
3. Click *Upload File*. Enter the name and path of the customization template in the input field.
4. Click *Upload File*.

Add customization provisioning information for each device

1. Sign in to *Cisco Unified CM Administration*.
2. Navigate to *Device > Phone*.
3. Fill in the **Customization Provisioning** fields in the product specific configuration section of the relevant devices:
  - *Customization File*: The customization template file name (for example: backup.zip) \*
  - *Customization Hash Type*: **SHA512**
  - *Customization Hash*: The SHA512 checksum for the customization template.

If these fields are not present, you must install a newer Device Package on CUCM.

4. Click *Save* and *Apply Config* to push the configuration to the devices.

\* If not using the TFTP Service, you must enter the complete URI for the customization template: <hostname>:<portnumber>/<path-and-filename>

For example:

- http://host:6970/backup.zip, or
- https://host:6971/backup.zip

### SHA512 checksum

**Tip!** You can find the SHA512 checksum of a file by restoring it to a device using its web interface.

1. Sign in to the web interface and navigate to *Maintenance > Backup and Restore*.
2. Choose the *Restore backup* tab.
3. Click *Browse...* and find the file you want to calculate the checksum for.

Then you can see the SHA512 checksum at the bottom of the page.

### CUCM documentation

► <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

## TMS provisioning of custom elements

A backup file, as described in the ► [Backup and restore configurations and custom elements](#) chapter, can be used as a *customization template* for multiple devices.

The backup file must be hosted on a custom web server that can be reached by the devices on HTTP or HTTPS.

When a device get information from TMS (TelePresence Management Suite) about the name and location of the backup file, the device will contact the server, download the file, and restore the custom elements.

### Create and apply a configuration template

1. Create a configurations template.
2. Add a custom command containing the following XML string in the configuration template:

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

where

*web-server-address*: The URI to the backup file (for example, <http://host/backup.zip>).

*checksum*: The SHA512 checksum of the backup file.

*origin*: **Provisioning**\*

3. Select the devices you want to push the configuration template to, and click [Set on systems](#).

Read the ► [Cisco TMS administrator guide](#) for details how to create TMS configurations templates and make custom commands.

### SHA512 checksum

**Tip!** You can find the SHA512 checksum of a file by restoring it to a device using its web interface.

1. Sign in to the web interface and navigate to [Maintenance > Backup and Restore](#).
2. Choose the [Restore backup](#) tab.
3. Click [Browse...](#) and find the file you want to calculate the checksum for.

Then you can see the SHA512 checksum at the bottom of the page.

\* If not setting this parameter to **Provisioning**, also configurations that are part of the backup file will be pushed to the device. If the backup file contains configurations that are specific to one device, for example static IP addresses, device name, and contact information, you may end up with devices that you cannot reach.

## 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, configurations, and custom elements of the device before you swap to the previously used software image.

### Back up log files, configurations and custom elements

1. Select the *Backup* tab.
2. Click [Download logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download backup](#) and follow the instructions to save the backup bundle 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 *OK* to confirm your choice, or *Cancel* if you have changed your mind.

Wait while the device resets. The device 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 device, switching to the previously used software image may help solving the problem.

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



## Factory reset the video conferencing device (page 1 of 3)

If there is a severe problem with the device, 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 device. Read about software swapping in the [► Revert to the previously used software image](#) chapter.

We recommend that you use the web interface or user interface to factory reset the device. If these interfaces are not available, use the reset pin-hole.

A factory reset implies:

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

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

**We recommend that you back up the log files, configurations, and custom elements of the device before you perform a factory reset; otherwise these data will be lost.**

## Factory reset the video conferencing device (page 2 of 3)

### Factory reset using the web interface

We recommend that you back up the log files and configuration of the device 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 device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

When the device has been successfully reset to factory settings, the *Setup assistant* starts with the *Welcome* screen.

### Factory reset from the user interface

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

1. Select the device name or address at the top of the user interface.
2. Select [Settings](#).
3. Select [Factory reset](#).
4. Select [Reset](#) to confirm your choice, or [Back](#) if you have changed your mind.
5. Wait while the device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

When the device has been successfully reset to factory settings, the *Setup assistant* starts with the *Welcome* screen.

### Back up log files, configurations, and custom elements

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

1. Select the *Backup* tab.
2. Click [Download logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download backup](#) and follow the instructions to save the backup bundle on your computer.

## Factory reset the video conferencing device (page 3 of 3)

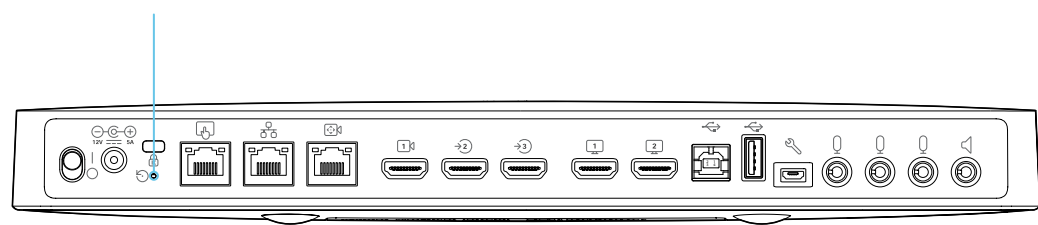
### Factory reset using the reset button

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

1. Locate the reset button (pin hole) at the rear side of the codec.
2. Use a paper clip (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 device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

When the device has been successfully reset to factory settings, the Setup assistant starts with the *Welcome* screen.

Reset button (pin hole)



## Factory reset Cisco Touch 10

**This chapter applies to the new Touch 10 controller that was launched late 2017 (Cisco Touch 10).** This device is identified by the logo on front, and fewer connectors at the back.

See the next page for the older version.

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 conferencing device) is reverted to factory defaults.



It is not possible to undo a factory reset.

1. Open the small cover at the rear to find the reset button.
2. Press and hold the reset button until the mute button at the front starts blinking (approximately 5 seconds). Then release the button.

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

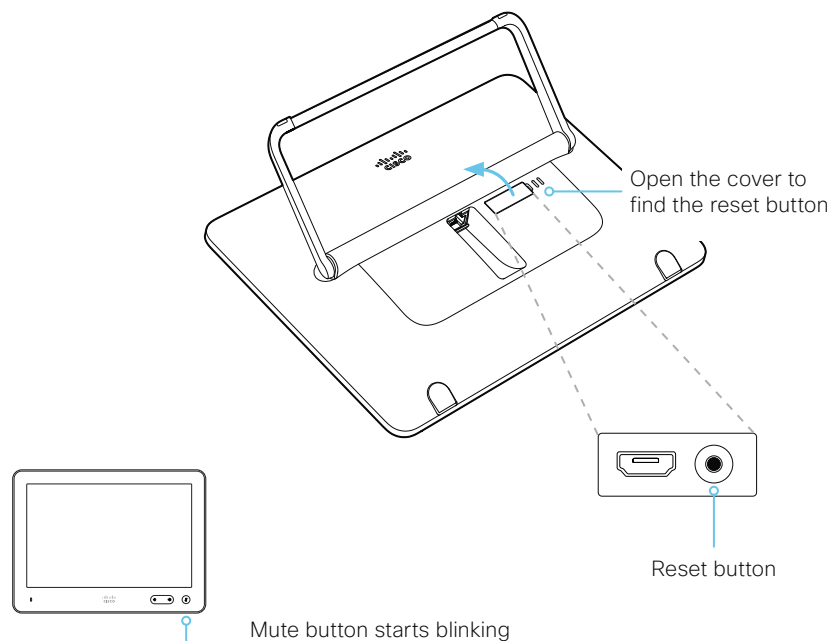
If Touch 10 is directly connected to the video conferencing device, it receives a new configuration automatically from the device.

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

### About pairing and how to connect Touch 10 to the video conferencing device

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

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



## Factory reset Cisco TelePresence Touch 10

**This chapter applies to the first Touch 10 controller (Cisco TelePresence Touch 10).** This device has no logo on front.

See the previous page for the newer version that was launched late 2017.

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 conferencing device) is reverted to factory defaults.



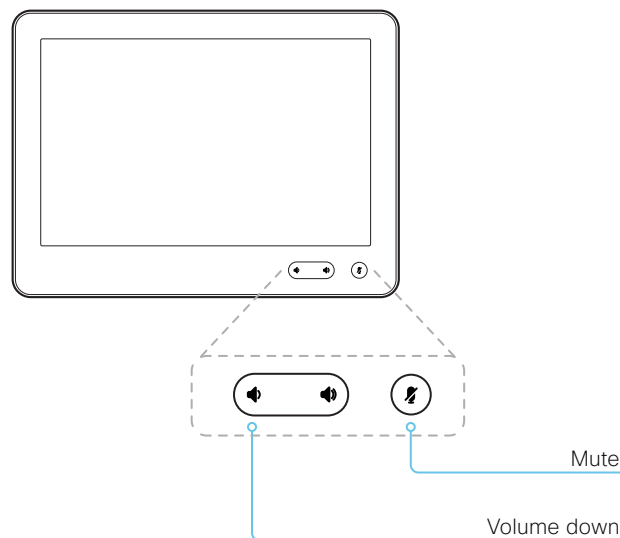
It is not possible to undo a factory reset.

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

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

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

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



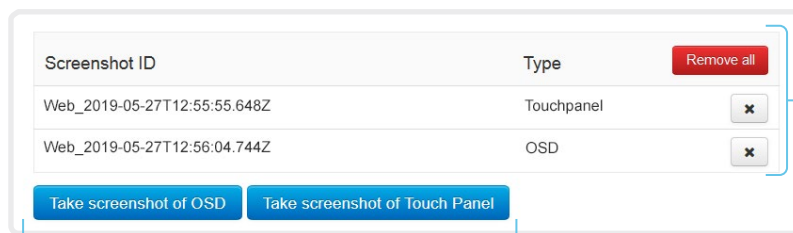
### About pairing and how to connect Touch 10 to the video conferencing device

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

Read about pairing and how to connect Touch 10 to the video conferencing device 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 main screen (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 device, and of the main screen with menus, indicators and messages (also know as *on-screen display*).

## Chapter 5

# Device settings

## Overview of the device settings

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

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



### How to find the IP address

1. Select the device name or address at the top of the user interface.
2. Select [Settings](#), followed by [About this device.d](#)

<b>Audio settings</b> .....	<b>126</b>
Audio DefaultVolume.....	126
Audio Input ARC [n] Mode.....	126
Audio Input HDMI [n] Level.....	126
Audio Input HDMI [n] Mode .....	126
Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo .....	127
Audio Input Microphone [n] EchoControl Dereverberation .....	127
Audio Input Microphone [n] EchoControl Mode .....	127
Audio Input Microphone [n] EchoControl NoiseReduction .....	127
Audio Input Microphone [n] Level.....	128
Audio Input Microphone [n] Mode.....	128
Audio KeyClickDetector Attenuate.....	128
Audio KeyClickDetector Enabled .....	128
Audio Microphones Mute Enabled.....	129
Audio Microphones PhantomPower .....	129
Audio Output HDMI [n] Mode .....	129
Audio Output InternalSpeaker Mode.....	129
Audio Output Line [n] Mode .....	129
Audio Output Line [n] OutputType .....	130
Audio SoundsAndAlerts RingTone.....	130
Audio SoundsAndAlerts RingVolume.....	130
Audio Ultrasound MaxVolume.....	130
Audio Ultrasound Mode .....	130
<b>CallHistory settings</b> .....	<b>131</b>
CallHistory Mode.....	131
<b>Cameras settings</b> .....	<b>132</b>
Cameras Camera [n] AssignedSerialNumber .....	132
Cameras Camera [n] Backlight DefaultMode .....	132
Cameras Camera [n] Brightness DefaultLevel .....	132
Cameras Camera [n] Brightness Mode.....	132
Cameras Camera [n] Focus Mode .....	133
Cameras Camera [n] Gamma Level .....	133
Cameras Camera [n] Gamma Mode.....	133
Cameras Camera [n] Mirror.....	133



Cameras Camera [n] Whitebalance Level.....	134	<b>FacilityService settings.....</b>	<b>142</b>
Cameras Camera [n] Whitebalance Mode.....	134	FacilityService Service [n] CallType.....	142
Cameras PowerLine Frequency.....	134	FacilityService Service [n] Name.....	142
Cameras PresenterTrack CameraPosition Pan.....	134	FacilityService Service [n] Number.....	142
Cameras PresenterTrack CameraPosition Tilt.....	134	FacilityService Service [n] Type.....	142
Cameras PresenterTrack CameraPosition Zoom.....	135	<b>H323 settings.....</b>	<b>143</b>
Cameras PresenterTrack Connector.....	135	H323 Authentication LoginName.....	143
Cameras PresenterTrack Enabled.....	135	H323 Authentication Mode.....	143
Cameras PresenterTrack PresenterDetectedStatus.....	135	H323 Authentication Password.....	143
Cameras PresenterTrack TriggerZone.....	135	H323 CallSetup Mode.....	143
Cameras SpeakerTrack Closeup.....	136	H323 Encryption KeySize.....	144
Cameras SpeakerTrack Mode.....	136	H323 Gatekeeper Address.....	144
Cameras SpeakerTrack Whiteboard Mode.....	136	H323 H323Alias E164.....	144
<b>Conference settings.....</b>	<b>137</b>	H323 H323Alias ID.....	144
Conference ActiveControl Mode.....	137	H323 NAT Address.....	145
Conference AutoAnswer Delay.....	137	H323 NAT Mode.....	144
Conference AutoAnswer Mode.....	137	H323 PortAllocation.....	145
Conference AutoAnswer Mute.....	137	<b>HttpClient settings.....</b>	<b>146</b>
Conference CallProtocolIPStack.....	137	HttpClient AllowHTTP.....	146
Conference DefaultCall Protocol.....	138	HttpClient AllowInsecureHTTPS.....	146
Conference DefaultCall Rate.....	138	HttpClient Mode.....	146
Conference DoNotDisturb DefaultTimeout.....	138	<b>HttpFeedback settings.....</b>	<b>147</b>
Conference Encryption Mode.....	138	HttpFeedback TlsVerify.....	147
Conference FarEndControl Mode.....	138	<b>Logging settings.....</b>	<b>148</b>
Conference FarEndControl SignalCapability.....	139	Logging Debug Wifi.....	148
Conference FarEndMessage Mode.....	139	Logging External Mode.....	148
Conference IncomingMultisiteCall Mode.....	141	Logging External Protocol.....	148
Conference MaxReceiveCallRate.....	139	Logging External Server Address.....	148
Conference MaxTotalReceiveCallRate.....	139	Logging External Server Port.....	148
Conference MaxTotalTransmitCallRate.....	140	Logging External TlsVerify.....	149
Conference MaxTransmitCallRate.....	139	Logging Internal Mode.....	149
Conference MicUnmuteOnDisconnect Mode.....	140	Logging Mode.....	149
Conference Multipoint Mode.....	140	<b>Macros settings.....</b>	<b>150</b>
Conference MultiStream Mode.....	141	Macros AutoStart.....	150
Conference Presentation OnPlacedOnHold.....	141	Macros Mode.....	150
Conference Presentation RelayQuality.....	141		
Conference VideoBandwidth Mode.....	141		

Macros UnresponsiveTimeout .....	150	<b>NetworkServices settings .....</b>	<b>159</b>
Macros XAPI Transport .....	150	NetworkServices CDP Mode .....	159
<b>Network settings .....</b>	<b>151</b>	NetworkServices H323 Mode .....	159
Network [n] DNS DNSSEC Mode .....	151	NetworkServices HTTP Mode .....	159
Network [n] DNS Domain Name .....	151	NetworkServices HTTP Proxy LoginName .....	159
Network [n] DNS Server [m] Address .....	151	NetworkServices HTTP Proxy Mode .....	160
Network [n] IEEE8021X AnonymousIdentity .....	152	NetworkServices HTTP Proxy PACUrl .....	160
Network [n] IEEE8021X Eap Md5 .....	153	NetworkServices HTTP Proxy Password .....	160
Network [n] IEEE8021X Eap Peap .....	153	NetworkServices HTTP Proxy Url .....	160
Network [n] IEEE8021X Eap Tls .....	153	NetworkServices HTTPS OCSP Mode .....	160
Network [n] IEEE8021X Eap Ttls .....	153	NetworkServices HTTPS OCSP URL .....	161
Network [n] IEEE8021X Identity .....	152	NetworkServices HTTPS Server MinimumTLSVersion .....	161
Network [n] IEEE8021X Mode .....	151	NetworkServices HTTPS StrictTransportSecurity .....	161
Network [n] IEEE8021X Password .....	152	NetworkServices HTTPS VerifyClientCertificate .....	161
Network [n] IEEE8021X TlsVerify .....	152	NetworkServices NTP Mode .....	161
Network [n] IEEE8021X UseClientCertificate .....	152	NetworkServices NTP Server [n] Address .....	162
Network [n] IPStack .....	153	NetworkServices NTP Server [n] Key .....	162
Network [n] IPv4 Address .....	154	NetworkServices NTP Server [n] KeyAlgorithn .....	162
Network [n] IPv4 Assignment .....	154	NetworkServices NTP Server [n] Keyld .....	162
Network [n] IPv4 Gateway .....	154	NetworkServices SIP Mode .....	162
Network [n] IPv4 SubnetMask .....	154	NetworkServices SNMP CommunityName .....	163
Network [n] IPv6 Address .....	155	NetworkServices SNMP Host [n] Address .....	163
Network [n] IPv6 Assignment .....	154	NetworkServices SNMP Mode .....	162
Network [n] IPv6 DHCPOptions .....	155	NetworkServices SNMP SystemContact .....	163
Network [n] IPv6 Gateway .....	155	NetworkServices SNMP SystemLocation .....	163
Network [n] MTU .....	155	NetworkServices SSH AllowPublicKey .....	163
Network [n] QoS Diffserv Audio .....	156	NetworkServices SSH HostKeyAlgorithm .....	163
Network [n] QoS Diffserv Data .....	156	NetworkServices SSH Mode .....	163
Network [n] QoS Diffserv ICMPv6 .....	157	NetworkServices UPnP Mode .....	164
Network [n] QoS Diffserv NTP .....	157	NetworkServices UPnP Timeout .....	164
Network [n] QoS Diffserv Signalling .....	156	NetworkServices Websocket .....	164
Network [n] QoS Diffserv Video .....	156	NetworkServices WelcomeText .....	164
Network [n] QoS Mode .....	155	NetworkServices Wifi Allowed .....	165
Network [n] RemoteAccess Allow .....	157	NetworkServices Wifi Enabled .....	165
Network [n] Speed .....	157	NetworkServices XMLAPI Mode .....	165
Network [n] TrafficControl Mode .....	158	<b>Peripherals settings .....</b>	<b>166</b>
Network [n] VLAN Voice Mode .....	158	Peripherals InputDevice Mode .....	166
Network [n] VLAN Voice VlanId .....	158	Peripherals Pairing CiscoTouchPanels EmcResilience .....	166
		Peripherals Pairing CiscoTouchPanels RemotePairing .....	166

Peripherals Profile Cameras .....	166	RTP Video Ports Range Start.....	177
Peripherals Profile ControlSystems .....	167	RTP Video Ports Range Stop.....	177
Peripherals Profile TouchPanels .....	167		
<b>Phonebook settings .....</b>	<b>168</b>	<b>Security settings .....</b>	<b>178</b>
Phonebook Server [n] ID .....	168	Security Audit Logging Mode .....	178
Phonebook Server [n] Pagination.....	168	Security Audit OnError Action.....	178
Phonebook Server [n] TlsVerify.....	168	Security Audit Server Address .....	178
Phonebook Server [n] Type.....	169	Security Audit Server Port .....	178
Phonebook Server [n] URL.....	169	Security Audit Server PortAssignment.....	179
		Security Fips Mode .....	179
<b>Provisioning settings.....</b>	<b>170</b>	Security Session FailedLoginsLockoutTime .....	179
Provisioning Connectivity.....	170	Security Session InactivityTimeout .....	179
Provisioning ExternalManager Address.....	170	Security Session MaxFailedLogins .....	179
Provisioning ExternalManager AlternateAddress.....	170	Security Session MaxSessionsPerUser.....	180
Provisioning ExternalManager Domain .....	171	Security Session MaxTotalSessions .....	180
Provisioning ExternalManager Path .....	171	Security Session ShowLastLogon .....	180
Provisioning ExternalManager Protocol.....	170		
Provisioning LoginName .....	171	<b>SerialPort settings .....</b>	<b>181</b>
Provisioning Mode .....	171	SerialPort BaudRate.....	181
Provisioning Password.....	172	SerialPort LoginRequired .....	181
Provisioning TlsVerify .....	172	SerialPort Mode .....	181
Provisioning WebexEdge .....	172		
		<b>SIP settings.....</b>	<b>182</b>
<b>Proximity settings .....</b>	<b>173</b>	SIP ANAT.....	182
Proximity AlternatePort Enabled .....	173	SIP Authentication Password.....	182
Proximity Mode .....	173	SIP Authentication UserName .....	182
Proximity Services CallControl .....	173	SIP DefaultTransport .....	182
Proximity Services ContentShare FromClients.....	174	SIP DisplayName.....	182
Proximity Services ContentShare ToClients .....	174	SIP Ice DefaultCandidate .....	183
		SIP Ice Mode.....	183
<b>RoomAnalytics settings .....</b>	<b>175</b>	SIP Line .....	183
RoomAnalytics AmbientNoiseEstimation Mode.....	175	SIP ListenPort .....	183
RoomAnalytics PeopleCountOutOfCall .....	175	SIP Mailbox .....	184
RoomAnalytics PeoplePresenceDetector.....	175	SIP MinimumTLSVersion .....	184
		SIP PreferredIPSignaling.....	184
<b>RoomReset settings.....</b>	<b>176</b>	SIP Proxy [n] Address.....	184
RoomReset Control.....	176	SIP TlsVerify .....	184
		SIP Turn DiscoverMode .....	185
<b>RTP settings.....</b>	<b>177</b>	SIP Turn DropRflx.....	185
RTP Ports Range Start.....	177	SIP Turn Password.....	185
RTP Ports Range Stop .....	177		

SIP Turn Server.....	185	UserInterface Features Share Start.....	195
SIP Turn UserName.....	185	UserInterface KeyTones Mode.....	194
SIP Type.....	185	UserInterface Language.....	195
SIP URI.....	186	UserInterface OSD EncryptionIndicator.....	196
<b>Standby settings.....</b>	<b>187</b>	UserInterface OSD HalfwakeMessage.....	196
Standby BootAction.....	187	UserInterface OSD Output.....	196
Standby Control.....	187	UserInterface Phonebook Mode.....	196
Standby Delay.....	187	UserInterface Security Mode.....	197
Standby Signage Audio.....	187	UserInterface SettingsMenu Mode.....	197
Standby Signage Mode.....	187	UserInterface SettingsMenu Visibility.....	197
Standby Signage RefreshInterval.....	188	UserInterface SoundEffects Mode.....	197
Standby Signage Url.....	188	UserInterface Wallpaper.....	198
Standby StandbyAction.....	188	<b>UserManagement settings.....</b>	<b>199</b>
Standby WakeupAction.....	188	UserManagement LDAP Admin Filter.....	199
Standby WakeupOnMotionDetection.....	188	UserManagement LDAP Admin Group.....	199
<b>SystemUnit settings.....</b>	<b>189</b>	UserManagement LDAP Attribute.....	199
SystemUnit CrashReporting Advanced.....	189	UserManagement LDAP BaseDN.....	199
SystemUnit CrashReporting Mode.....	189	UserManagement LDAP Encryption.....	199
SystemUnit CrashReporting Url.....	189	UserManagement LDAP MinimumTLSVersion.....	200
SystemUnit Name.....	189	UserManagement LDAP Mode.....	200
<b>Time settings.....</b>	<b>190</b>	UserManagement LDAP Server Address.....	200
Time DateFormat.....	190	UserManagement LDAP Server Port.....	200
Time TimeFormat.....	190	UserManagement LDAP VerifyServerCertificate.....	200
Time Zone.....	191	UserManagement PasswordPolicy Complexity MinimumDigits.....	201
<b>UserInterface settings.....</b>	<b>193</b>	UserManagement PasswordPolicy Complexity MinimumLength.....	201
UserInterface Accessibility IncomingCallNotification.....	193	UserManagement PasswordPolicy Complexity MinimumLowercase.....	201
UserInterface Assistant Mode.....	193	UserManagement PasswordPolicy Complexity MinimumSpecial.....	201
UserInterface Assistant Mode.....	193	UserManagement PasswordPolicy Complexity MinimumUppercase.....	202
UserInterface Branding AwakeBranding Colors.....	193	UserManagement PasswordPolicy MaxLifetime.....	202
UserInterface ContactInfo Type.....	194	UserManagement PasswordPolicy ReuseLimit.....	202
UserInterface CustomMessage.....	194	<b>Video settings.....</b>	<b>203</b>
UserInterface Features Call End.....	194	Video ActiveSpeaker DefaultPIPPosition.....	203
UserInterface Features Call JoinWebex.....	195	Video DefaultLayoutFamily Local.....	203
UserInterface Features Call MidCallControls.....	194	Video DefaultLayoutFamily Remote.....	204
UserInterface Features Call Start.....	195	Video DefaultMainSource.....	204
UserInterface Features Call VideoMute.....	195	Video Input Connector [n] CameraControl Camerald.....	204
UserInterface Features HideAll.....	195	Video Input Connector [n] CameraControl Mode.....	204
		Video Input Connector [n] CEC Mode.....	205

Video Input Connector [n] HDCP Mode .....	205
Video Input Connector [n] InputSourceType .....	205
Video Input Connector [n] Name.....	205
Video Input Connector [n] OptimalDefinition Profile.....	206
Video Input Connector [n] OptimalDefinition Threshold60fps .....	206
Video Input Connector [n] PreferredResolution .....	206
Video Input Connector [n] PresentationSelection .....	207
Video Input Connector [n] Quality .....	207
Video Input Connector [n] RGBQuantizationRange .....	207
Video Input Connector [n] Visibility .....	208
Video Monitors.....	208
Video Output Connector [n] CEC Mode.....	208
Video Output Connector [n] Location HorizontalOffset .....	209
Video Output Connector [n] Location VerticalOffset.....	209
Video Output Connector [n] MonitorRole .....	210
Video Output Connector [n] Resolution .....	210
Video Output Connector [n] RGBQuantizationRange.....	211
Video Presentation DefaultPIPPosition .....	211
Video Presentation DefaultSource.....	211
Video Presentation Priority .....	211
Video Selfview Default FullscreenMode .....	212
Video Selfview Default Mode.....	212
Video Selfview Default OnMonitorRole.....	212
Video Selfview Default PIPPosition.....	212
Video Selfview OnCall Duration .....	213
Video Selfview OnCall Mode .....	213
<b>WebEngine settings .....</b>	<b>214</b>
WebEngine Mode.....	214
WebEngine RemoteDebugging.....	214
<b>Experimental settings .....</b>	<b>215</b>

## 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 conferencing device. Use the controls on the user interface to change the volume while it is running. You may also use API commands (xCommand Audio Volume) to change the volume while the device is running, and to reset to default value.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

Range: 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 Input ARC [n] Mode

n: 1..1

Each HDMI output has an associated audio return channel (ARC). You can use the ARC to send audio from a screen or TV, which is connected to the HDMI output, to the video conferencing device. You can decide for each HDMI output connector (n) separately, whether or not to allow audio transmission.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the ARC channel of HDMI output n (audio is not sent to the video conferencing device).

On: Enable the ARC channel of HDMI output n (audio is sent to the video conferencing device).

### Audio Input HDMI [n] Level

n: 2..3

Set the gain on the HDMI input connector. The gain can be tuned in steps of 1 dB.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (-24..0)

Range: Select the gain in decibel (dB).

### Audio Input HDMI [n] Mode

n: 2..3

Define if the audio on the HDMI input connector shall be enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable audio on the HDMI input.

On: Enable audio on the HDMI input.

## Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo

n: 2..3

Use this setting to decide whether to stop the audio playback of a connected presentation source if that presentation source is not currently shown on-screen, or to always playback the audio as long as the presentation source is connected.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Audio is played, locally and to far end, as long as a presentation source is connected; you do not have to present the HDMI input source.

On: Audio is played, locally and to far end, only when the connected presentation source is shown on-screen.

## Audio Input Microphone [n] EchoControl Mode

n: 1..3

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, INTEGRATOR

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 [n] EchoControl Dereverberation

n: 1..3

The video conferencing device 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, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

## Audio Input Microphone [n] EchoControl NoiseReduction

n: 1..3

The video conferencing device 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, INTEGRATOR

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 [n] Level

n: 1..3

Set the gain on the Microphone input connector. The gain should be adjusted to suit the output level of the connected audio source. The gain can be tuned in steps of 1 dB.

If the gain is set too high, the audio signal will be clipped. If the gain is set too low, the audio signal-to-noise ratio will be degraded; however, this is usually preferable to clipping.

Note that unprocessed speech signals typically contain significant level variations, making it very important to allow for sufficient signal headroom.

The maximum input level with 0 dB gain is -18 dBu.

Example: If your microphone has a maximum output level of -40 dBu, then you should set the gain to -18 dBu - (-40 dBu) = 22 dB.

Requires user role: ADMIN, INTEGRATOR

Default value: 14

Value space: Integer (0..24)

Range: Select the gain in decibel (dB).

## Audio Input Microphone [n] Mode

n: 1..3

Disable or enable audio on the microphone connector.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the audio input microphone connector.

On: Enable the audio input microphone connector.

## Audio KeyClickDetector Attenuate

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb the other participants. If the participant types on the keyboard and speaks at the same time the microphone signal will not be attenuated. Requires that the Audio KeyClickDetector Enabled setting is set to On.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: True

Value space: False/True

False: The attenuation of the microphone signal is disabled.

True: The device attenuates the microphone signal if clicking noise from keyboards is detected. If voice or voice + keyboard clicks are detected the microphone signal is not attenuated.

## Audio KeyClickDetector Enabled

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb other participants. To enable attenuation on the microphone signal, set the Audio KeyClickDetector Attenuate to On.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: True

Value space: False/True

False: The key click detection is disabled.

True: The device will detect clicking noise from keyboards.



## Audio Microphones Mute Enabled

Define the microphone mute behavior on the device.

Requires user role: ADMIN, INTEGRATOR

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 device and is to be available when the device is not in a call. When set to InCallOnly this will prevent the audio-system from being muted by mistake.

## Audio Microphones PhantomPower

Define whether or not to have phantom power (11 V +/- 1 V) on the microphone input.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the phantom power on the microphone input. Use this when connecting to equipment that do not need phantom power, such as external mixers.

On: Enable the phantom power on the microphone input. Use this when connecting directly to microphones that require phantom power, including the Cisco Table Microphone and Cisco Ceiling Microphone.

## Audio Output HDMI [n] Mode

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The connector will not be used for audio out.

On: The connector will be used for audio out.

## Audio Output InternalSpeaker Mode

Define whether or not to use the camera's integrated speakers. The device must be connected to a Quad Camera for this setting to apply.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the device's integrated speakers.

On: Enable the device's integrated speakers.

## Audio Output Line [n] Mode

n: 1..1

Define the mode for the audio line output.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the audio line output.

On: Enable the audio line output.

## Audio Output Line [n] OutputType

n: 1..1

The output type should be set to match the connected device.

Requires user role: ADMIN, INTEGRATOR

Default value: Loudspeaker

Value space: LineOut/Loudspeaker/Recorder

**Loudspeaker:** Use Loudspeaker if a loudspeaker is connected to the line output. In this mode, the output level on that connector follows the master volume control, and the output signal includes all system sounds (ringtones, webex assistant etc.).

**Recorder:** Use Recorder if a recorder is connected to the line output. In this mode, the output level is fixed, and system sounds are not included. What is included is the sound from local presentation sources, the local microphones as well as any far end sources.

**LineOut:** Use LineOut for other devices. In this mode, the internal speaker will play full range audio. The output level is fixed, and system sounds are not included. What is included is the sound from local presentation sources, as well as any far end sources.

## Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: ADMIN, INTEGRATOR, 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, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

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

## Audio Ultrasound Mode

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN, INTEGRATOR

Default value: Dynamic

Value space: Dynamic/Static

**Dynamic:** The device adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Audio Ultrasound Volume MaxVolume setting.

**Static:** Use only if advised by Cisco.

## Audio Ultrasound MaxVolume

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing messages.

The Audio Ultrasound MaxVolume and Proximity Mode settings only affect ultrasound pairing messages. See the RoomAnalytics PeoplePresenceDetector and Standby WakeupOnMotionDetection settings for information about the use of ultrasound in presence and motion detection.

Requires user role: ADMIN, INTEGRATOR

Default value: 70

Value space: Integer (0..90)

Select a value in the specified range. If set to 0, ultrasound pairing messages are not emitted.

## 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, INTEGRATOR

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 [n] AssignedSerialNumber

n: 1..3

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

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

Typical situations where the video conferencing device does not receive EDID information are: when you connect a Cisco TelePresence Precision 60 camera using 3G-SDI, or when you use an HDMI repeater that does not pass on EDID information.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 20)

The camera's serial number.

### Cameras Camera [n] Backlight DefaultMode

n: 1..3

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.

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

### Cameras Camera [n] Brightness Mode

n: 1..3

Define the camera brightness mode.

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

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

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

### Cameras Camera [n] Brightness DefaultLevel

n: 1..3

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

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: 20

Value space: Integer (1..31)

The brightness level.

## Cameras Camera [n] Focus Mode

n: 1..3

Define the camera focus mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/AutoLimited/Manual

Auto: Cisco TelePresence Precision 60 camera: The camera will do continuous auto focusing. It will, more specifically, run auto focus once a call is connected, after pan, tilt, zoom have changed, and generally when the camera identifies a change in the scene.

Auto: Cisco Quad Camera: The camera will do single shot auto focusing once a call is connected and when the view has changed.

AutoLimited: Cisco TelePresence Precision 60 camera. In most cases this mode will operate the same way as Auto. In some cases AutoLimited will reduce the focus hunting that may occur. Problematic scenes have large areas with no or low contrast, for instance a painted wall with no details, or maybe a partly empty whiteboard. There's a slightly higher chance of background focus with this mode, compared to Auto.

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

## Cameras Camera [n] Gamma Mode

n: 1..3

This setting enables gamma corrections. Gamma describes the nonlinear relationship between image pixels and monitor brightness.

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: Auto is the default and the recommended setting.

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

## Cameras Camera [n] Gamma Level

n: 1..3

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

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (0..7)

Define the gamma level.

## Cameras Camera [n] Mirror

n: 1..3

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. This setting is not applicable when your video conferencing device has a Cisco Quad Camera or when speaker tracking is on.

Requires user role: ADMIN, INTEGRATOR

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 [n] Whitebalance Mode

n: 1..3

Define the camera white balance mode.

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

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 [n] Whitebalance Level

n: 1..3

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

Not applicable if you have a Cisco Quad Camera, because this camera automatically adjusts itself based on the room lighting conditions.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: Integer (1..16)

The white balance level.

## Cameras PowerLine Frequency

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: 50Hz/60Hz/Auto

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

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

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

## Cameras PresenterTrack CameraPosition Pan

Define the pan position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (-65535..65535)

The pan position.

## Cameras PresenterTrack CameraPosition Tilt

Define the tilt position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (-65535..65535)

The tilt position.

## Cameras PresenterTrack CameraPosition Zoom

Define the zoom position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (-65535..65535)

The zoom position.

## Cameras PresenterTrack Connector

Define which video input connector the presenter tracking camera is connected to. Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: Integer (1..3)

The video input connector.

## Cameras PresenterTrack Enabled

Define whether or not the PresenterTrack feature is available for use. Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: False

Value space: False/True

False: The PresenterTrack feature is disabled.

True: The PresenterTrack feature is available for use.

## Cameras PresenterTrack PresenterDetectedStatus

Define whether to enable or disable automatic switching between the Remote Presenter and Local Presenter modes in the Classroom scenario (Room Type templates). Automatic switching implies that the device switches to Local Presenter mode when a person is detected in the PresenterTrack trigger zone, and that the device switches back to the Remote Presenter mode when the local presenter leaves the stage.

If this setting is enabled, the Cameras PresenterTrack PresenterDetected status will be updated when a new person enters the trigger zone.

Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: Enabled

Value space: Disabled/Enabled

Disabled: No automatic switching between modes.

Enabled: Automatic switching between the Local Presenter and Remote Presenter modes.

## Cameras PresenterTrack TriggerZone

Define the trigger zone, which corresponds to the area where a person's face must be detected for presenter tracking to start.

The format is a string of x and y coordinate pairs: "x1,y1,...xn,yn", where the range of x is (0,1920) and y is (0,1080). Two coordinate pairs define the upper left and lower right corner of a rectangular trigger zone. More than two coordinate pairs define the vertices of a polygonal trigger zone.

Only the Precision 60 camera supports presenter tracking.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0..255)

The coordinates for the trigger zone.

## Cameras SpeakerTrack Mode

This setting applies only when using a camera with support for speaker tracking.

For video conferencing devices with Cisco Quad Camera: Speaker tracking uses automatic camera framing to select the best camera view based on where people are in the room.

The Quad Camera uses an audio tracking technique that finds and captures a close-up of the active speaker.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Off

Auto: Speaker tracking is switched on. The device will detect people in the room and automatically select the best camera framing. Users can switch speaker track on or off instantly in the camera control panel on the Touch controller, but the feature is switched back on after each call so that the device is ready for the next user.

Off: Speaker tracking is switched off.

## Cameras SpeakerTrack Closeup

This setting applies only when the Cameras SpeakerTrack Mode is set to Auto.

When the closeup functionality is turned on, the device will detect that a person is speaking and select the best framing to cover that person. This is called a closeup and may not include all the persons in the room. If you want all the persons in the room to be in the picture at all times you can turn off the closeup functionality.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Auto

Value space: Auto/Off/On

Auto: The device will zoom in on the person speaking.

Off: The device will keep all the persons in the room in the camera framing at all times.

On: The device will zoom in on the person speaking.

## Cameras SpeakerTrack Whiteboard Mode

This setting applies only when using a camera with support for speaker tracking.

The Snap to Whiteboard feature extends the speaker tracking functionality, thus you need a camera that supports speaker tracking. When a presenter is standing next to the whiteboard, the camera will capture both the presenter and the whiteboard if the Snap to Whiteboard feature is enabled. If the feature is disabled, only the presenter will be captured. The Snap to Whiteboard feature is set up from the Touch controller or web interface.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

Off: The Snap to Whiteboard feature is disabled.

On: The Snap to Whiteboard feature is enabled.



## Conference settings

### Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server or Cisco Meeting Server using the video conferencing device'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 device 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 can answer incoming calls manually by tapping Answer on the Touch controller.
- On: The device automatically answers incoming calls, except if you are already in a call. You can 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 device. 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 device should enable IPv4, IPv6, or dual IP stack on the call protocol (SIP, H323).

Requires user role: ADMIN

Default value: Dual

Value space: Dual/IPv4/IPv6

- Dual: Enables both IPv4 and IPv6 for the call protocol.
- IPv4: When set to IPv4, the call protocol will use IPv4.
- IPv6: When set to IPv6, the call protocol will use IPv6.

## Conference DefaultCall Protocol

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

Requires user role: ADMIN

Default value: Auto

Value space: Auto/H320/H323/Sip/Spark

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

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

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

Sip: All calls are set up as SIP calls.

Spark: Reserved for Webex registered devices. Do not use.

## Conference DefaultCall Rate

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

Requires user role: ADMIN, INTEGRATOR

Default value: 6000

Value space: Integer (64..6000)

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.

Requires user role: ADMIN, INTEGRATOR

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 device, the encryption mode is always Off.

Requires user role: ADMIN

Default value: BestEffort

Value space: Off/On/BestEffort

Off: The device will not use encryption.

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

BestEffort: The device will use encryption whenever possible.

> In Point to point calls: If the far end device 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 FarEndMessage Mode

Toggle whether it is allowed to send data between two devices in a point-to-point call, for use with control systems or macros. Works with SIP calls only. This setting will enable/disable the use of the xCommand Call FarEndMessage Send command.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: It is not possible to send messages between two devices.

On: It is possible to send messages between two devices in a point-to-point call.

## Conference MaxReceiveCallRate

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum receive call rate (kbps).

## Conference MaxTransmitCallRate

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum transmitt call rate (kbps).

## Conference MaxTotalReceiveCallRate

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

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

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum receive call rate (kbps).

## Conference MaxTotalTransmitCallRate

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

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

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

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 device for the next user.

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

On: Unmute the microphones after the call is disconnected.

## Conference Multipoint Mode

Define how to expand a point-to-point video call (a call involving only two parties) into a multipoint conference with more participants (ad hoc conferences). Both the built-in MultiSite feature, which relies only on local resources, and different solutions based on centralized infrastructure (multipoint control units – MCUs) are available.

The MultiSite feature is an upgrade option and may not be available on all devices. The MultiSite option key must be installed on the device.

If registered to a Cisco TelePresence Video Communication Server (VCS), the device can use MultiSite when calling other video devices. If registered to a Cisco Unified Communications Manager (CUCM) version 8.6.2 or newer, the device can use either a CUCM conference bridge, or the device's own built-in MultiSite feature. Which option to use, is set-up by CUCM.

In either case, multiparty conferences may be set up via an MCU if you call an MCU that allows devices to add participants to a conference (Direct Remote Add).

Requires user role: ADMIN

Default value: Auto

Value space: Auto/CUCMMediaResourceGroupList/MultiSite/Off

Auto: The multipoint method is selected automatically.

Multiparty conferences are set up using the built-in MultiSite feature, provided that the MultiSite option key is installed on the device, and that you are calling another video device (not an MCU). Only the MultiSite host can add participants. This prevents cascaded conferences. If the device doesn't have the MultiSite option key, you cannot call more than one video device on video. You may add one extra participant on audio-only.

Regardless of the MultiSite option key, multiparty conferences may be set up via an MCU if you call an MCU that allows devices to add participants to a conference (Direct Remote Add).

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

MultiSite: Multiparty conferences are set up using the built-in MultiSite feature, provided that the MultiSite option key is installed on the device. If the device doesn't have the MultiSite option key, you cannot call more than one device on video. You may add one extra device on audio-only.

Off: You cannot call more than one device on video, but you may add one extra device on audio-only. Multiparty conferences may be set up via an MCU if you call an MCU that allows devices to add participants to a conference (Direct Remote Add).

## Conference MultiStream Mode

The device supports multistream video for conferences.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off

Auto: Multistream will be used when the conference infrastructure supports the feature.

Minimum versions required: CMS 2.2, CUCM 11.5, VCS X8.7.

Off: Multistream is disabled.

## Conference IncomingMultisiteCall Mode

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

Requires user role: ADMIN

Default value: Allow

Value space: Allow/Deny

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

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

## Conference Presentation 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: NoAction/Stop

NoAction: The device 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.

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

## Conference Presentation RelayQuality

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

Requires user role: ADMIN

Default value: Sharpness

Value space: Motion/Sharpness

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

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

## Conference 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.

## FacilityService settings

### FacilityService Service [n] Type

n: 1..5

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. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

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 [n] Name

n: 1..5

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. The name will show on the facility service call button, which appears when you tap the question mark icon in the top bar. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

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

Value space: String (0, 1024)

The name of the facility service.

### FacilityService Service [n] Number

n: 1..5

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. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 1024)

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

### FacilityService Service [n] CallType

n: 1..5

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. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

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 device 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 device will try to authenticate itself to the gatekeeper. Requires the H323 Authentication LoginName and H323 Authentication Password settings to be defined on both the device and the Gatekeeper.

### H323 Authentication LoginName

The device 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 device to the H.323 Gatekeeper, i.e. the device is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the device 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 device 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 device to the H.323 Gatekeeper, i.e. the device is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the device 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 device 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: Max1024bit/Min1024bit/Min2048bit

Max1024bit: The maximum size is 1024 bit.

Min1024bit: The minimum 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 device, 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 device 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 device (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 device 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 devices on the LAN as well as devices on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.

Off: The device will signal the real IP address.

On: The device 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 video conferencing device. Note that NAT cannot be used when registered to a gatekeeper.

In the router, the following ports must be routed to the video conferencing device'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].

## HttpClient settings

### HttpClient Mode

Allow or prohibit communication with an external HTTP(S) server using HTTP(S) requests and responses.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The video conferencing device cannot communicate with an external HTTP(S) server.

On: The video conferencing device is allowed to communicate with an external HTTP(S) server.

### HttpClient AllowHTTP

The HttpClient Mode setting is used to allow or prohibit communication with an external HTTP(S) server. The Mode setting does not distinguish between HTTP and HTTPS. You must use the HttpClient AllowHTTP setting to further allow or prohibit the use of HTTP.

Requires user role: ADMIN

Default value: True

Value space: False/True

False: The video conferencing device can communicate only over HTTPS.

True: The video conferencing device can communicate over both HTTPS and HTTP.

### HttpClient AllowInsecureHTTPS

You can choose whether or not to allow the video conferencing device to communicate with a server over HTTPS without checking the server's certificate first.

Even if the device is allowed to skip the certificate validation process, it doesn't automatically do it. You must specifically set the AllowInsecureHTTPS parameter in each xCommand HttpClient command for data to be exchanged with the server without certificate validation.

Requires user role: ADMIN

Default value: False

Value space: False/True

False: The device always checks that the HTTPS server has a valid certificate. No communication with the server takes place if the certificate validation fails.

True: The device is allowed to skip the certificate validation process before communicating with the server.

## HttpFeedback settings

### HttpFeedback TlsVerify

This setting applies when a video conferencing device connects to an HTTPS server for arbitrary HTTPS communication (refer to the HttpClient Post/Put/Patch/Get/Delete commands). For phone book, provisioning, and external logging servers, see the Phonebook Server 1 TlsVerify, Provisioning TlsVerify, and Logging External TlsVerify settings.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.

## Logging settings

### Logging Debug Wifi

When this option is enabled, the device logs more information about the set-up and maintenance of the Wi-Fi connection between the device and the access point. This may be useful when you are troubleshooting Wi-Fi connection issues. We recommend that this setting is Off if the Wi-Fi connection is working as expected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Logging only basic Wi-Fi information.

On: Logging a large amount of information about the Wi-Fi connection.

### Logging External Mode

Determine whether or not to store the device logs on a remote syslog server. This setting has no effect if the Logging Mode setting is set to Off.

You must enter the address of the remote server in the Logging External Server Address setting. Unless otherwise specified in the Logging External Server Port setting, the standard syslog port is used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Device logs will not be stored on the remote syslog server.

On: Device logs will be stored on the 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, the device 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 device uses the standard syslog port.

## Logging External TlsVerify

This setting applies when a video conferencing device connects to a remote syslog server. It applies to both regular logging (refer to the Logging External Mode setting) and audit logging (refer to the Security Audit Logging Mode setting).

Before establishing a connection between the device and the syslog server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

The minimum TLS (Transport Layer Security) version for the syslog connection is 1.1.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The device doesn't check the certificate of the syslog server.

On: The device checks if the certificate of the syslog server can be trusted. If not, the connection between the device and the server is not established.

## Logging Internal Mode

Determine whether or not to store the system logs on the device (local files). These are the files that you get when you download the log bundles from the device. This setting has no effect if the Logging Mode setting is set to Off.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: System logs will not be stored on the device.

On: System logs will be stored on the device.

## Logging Mode

Define the logging mode for the device (syslog service). When disabled, the syslog service does not start, and most of the system and audit 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.

## Macros settings

### Macros Mode

Macros allow you to write snippets of JavaScript code that can automate parts of your video conferencing device, thus creating custom behavior. Use of macros is disabled by default, but the first time you open the Macro Editor you will be asked whether to enable use of macros on the device. Use this setting when you want to manually enable, or to permanently disable the use of macros on the device. You can disable the use of macros within the Macro Editor. But this will not permanently disable macros from running, because every time the device is reset the macros will be re-enabled automatically.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Permanently disable the use of macros on this device.

On: Enable the use of macros on this device.

### Macros AutoStart

All the macros run in a single process on the video conferencing device, called the macro runtime. It should be running by default, but you can choose to stop and start it manually. If you restart the device, the runtime will automatically start again if auto start is enabled.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The macro runtime will not start automatically after a restart of the device.

On: The macro runtime will start automatically after a restart of the device.

### Macros UnresponsiveTimeout

Macros are continuously monitored to detect unresponsive code. Unresponsive macros are typically a sign of a programming error, but occasionally it might be due to limited system resources. Increasing the value allows macros to run for longer without being terminated, while decreasing the value ensures that faulty macros do not consume system resources.

Requires user role: ADMIN

Default value: 5

Value space: Integer (0..65535)

Set the number of seconds before terminating an unresponsive macro. The value 0 disables the check altogether.

### Macros XAPI Transport

Set the xAPI transport method used in the macro system. WebSockets are to be considered as functional as t-shell but may be more unstable. This setting is exposed to allow early adoption and futureproofing of WebSockets.

Prior to software version CE9.10 the xAPI transport method was always t-shell.

Requires user role: ADMIN

Default value: TSH

Value space: TSH/WebSocket

TSH: The xAPI transport method for macros is t-shell.

WebSocket: The xAPI transport method for macros is WebSockets.

## Network settings

### Network [n] DNS DNSSEC Mode

n: 1..1

Domain Name System Security extensions (DNSSEC) is a set of extensions to DNS. It is used to authenticate DNS replies for zones that are signed. It will still allow unsigned zones.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable Domain Name System Security Extensions.

On: Enable Domain Name System Security Extensions.

### Network [n] DNS Domain Name

n: 1..1

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 [n] DNS Server [m] Address

n: 1..1

m: 1..3

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 [n] IEEE8021X Mode

n: 1..1

The device 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.

On: The 802.1X authentication is enabled.

## Network [n] IEEE8021X TlsVerify

n: 1..1

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 conferencing device. 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 device.

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 [n] IEEE8021X UseClientCertificate

n: 1..1

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video conferencing device. 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 conferencing device) will perform a mutual authentication TLS handshake with the server.

## Network [n] IEEE8021X Identity

n: 1..1

Define the username for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The username for 802.1X authentication.

## Network [n] IEEE8021X Password

n: 1..1

Define the password for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 50)

The password for 802.1X authentication.

## Network [n] IEEE8021X AnonymousIdentity

n: 1..1

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 [n] IEEE8021X Eap Md5

n: 1..1

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.

## Network [n] IEEE8021X Eap Ttls

n: 1..1

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.

## Network [n] IEEE8021X Eap Tls

n: 1..1

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.

## Network [n] IEEE8021X Eap Peap

n: 1..1

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.

## Network [n] IPStack

n: 1..1

Select if the device 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 device will use IPv4 on the network interface.

IPv6: When set to IPv6, the device will use IPv6 on the network interface.

## Network [n] IPv4 Assignment

n: 1..1

Define how the device will obtain its IPv4 address, subnet mask and gateway address. When using DHCP for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

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 device addresses are automatically assigned by the DHCP server.

## Network [n] IPv4 Address

n: 1..1

Define the static IPv4 network address for the device. 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 [n] IPv4 Gateway

n: 1..1

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 [n] IPv4 SubnetMask

n: 1..1

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 [n] IPv6 Assignment

n: 1..1

Define how the device will obtain its IPv6 address and the default gateway address.

When using DHCPv6 for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

Requires user role: ADMIN, USER

Default value: Autoconf

Value space: Static/DHCPv6/Autoconf

Static: The device 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 [n] IPv6 Address

n: 1..1

Define the static IPv6 network address for the device. 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 [n] IPv6 Gateway

n: 1..1

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 [n] IPv6 DHCPOptions

n: 1..1

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 [n] MTU

n: 1..1

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 [n] QoS Mode

n: 1..1

The QoS (Quality of Service) is a method which handles the priority of audio, video and other data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic. It provides QoS priorities on IP networks.

Requires user role: ADMIN, USER

Default value: Diffserv

Value space: Off/Diffserv

Off: No QoS method is used.

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 [n] QoS Diffserv Audio

n: 1..1

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Audio packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use EF for Audio. EF equals the decimal value 46.

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. 0 means "best-effort".

## Network [n] QoS Diffserv Video

n: 1..1

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets of the presentation channel (shared content) are also in the Video packet category. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use AF41 for Video. AF41 equals the decimal value 34.

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. 0 means "best-effort".

## Network [n] QoS Diffserv Data

n: 1..1

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Data packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use AF41 for Data. AF41 equals the decimal value 34.

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. 0 means "best-effort".

## Network [n] QoS Diffserv Signalling

n: 1..1

This setting takes effect only 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 traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use CS3 for Signalling. CS3 equals the decimal value 24.

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. 0 means "best-effort".

## Network [n] QoS Diffserv ICMPv6

n: 1..1

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority ICMPv6 packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use 0 for ICMPv6.

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. 0 means "best effort".

## Network [n] QoS Diffserv NTP

n: 1..1

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority NTP packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use 0 for NTP.

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. 0 means "best-effort".

## Network [n] RemoteAccess Allow

n: 1..1

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the device from SSH/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 [n] Speed

n: 1..1

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 auto-negotiation, make sure that the speed you choose is supported by the closest switch in your network infrastructure.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/10half/10full/100half/100full/1000full

Auto: Auto-negotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

1000full: Force link to 1 Gbps full-duplex.

## Network [n] TrafficControl Mode

n: 1..1

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 [n] VLAN Voice Mode

n: 1..1

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 [n] VLAN Voice VlanId

n: 1..1

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 device 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 device 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.

### NetworkServices HTTP Mode

Define whether or not to allow access to the device using the HTTP or HTTPS (HTTP Secure) protocols. Note that the device's web interface use HTTP or HTTPS. If this setting is switched Off, you cannot use the web interface.

For additional security (encryption and decryption of requests and pages that are returned by the web server), allow only HTTPS.

Note: The default value is HTTP+HTTPS for devices that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the device has not been factory reset after the upgrade.

Requires user role: ADMIN

Default value: HTTPS (changed from HTTP+HTTPS to HTTPS in CE9.4)

Value space: Off/HTTP+HTTPS/HTTPS

Off: Access to the device not allowed via HTTP or HTTPS.

HTTP+HTTPS: Access to the device allowed via both HTTP and HTTPS.

HTTPS: Access to the device allowed via HTTPS, but not via HTTP.

### NetworkServices HTTP Proxy LoginName

This is the username part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 80)

The authentication login name.

## NetworkServices HTTP Proxy Password

This is the password part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The authentication password.

## NetworkServices HTTP Proxy Mode

You can configure a device that is registered to the Cisco Webex cloud service to use a proxy server for HTTPS and WebSocket traffic. The HTTP proxy for Cisco Webex can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

If the device is registered to an on-premise service such as CUCM or VCS, keep this setting Off.

Requires user role: ADMIN, USER

Default value: Off

Value space: Manual/Off/PACUrl/WPAD

Manual: Enter the address of the proxy server in the NetworkServices HTTP Proxy URL setting. Optionally, also add the HTTP proxy login name and password in the NetworkServices HTTP Proxy LoginName/Password settings.

Off: The HTTP proxy mode is turned off.

PACUrl: The HTTP proxy is auto-configured. You must enter the URL for the PAC (Proxy Auto Configuration) script in the NetworkServices HTTP Proxy PACUrl setting.

WPAD: With WPAD (Web Proxy Auto Discovery) the HTTP proxy is fully automated and auto-configured.

## NetworkServices HTTP Proxy Url

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

The URL of the HTTP proxy server.

## NetworkServices HTTP Proxy PACUrl

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

The URL of the PAC (Proxy Auto Configuration) script.

## 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 HTTPS Server MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.1

Value space: TLSv1.1/TLSv1.2

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

## NetworkServices HTTPS StrictTransportSecurity

The HTTP Strict Transport Security header lets a web site inform the browser that it should never load the site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

## NetworkServices HTTPS VerifyClientCertificate

When the video conferencing device connects to an HTTPS client (like a web browser), the client can be asked to present a certificate to the video conferencing device 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 device in advance.

## NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the device'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 device 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 device will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The device will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

## NetworkServices NTP Server [n] Address

n: 1..3

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 NTP Server [n] Key

n: 1..3

To make sure that the NTP information comes from a trusted source, the video conferencing device must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 2045)

The key, which is part of the ID/key pair that the NTP source uses.

## NetworkServices NTP Server [n] KeyId

n: 1..3

To make sure that the NTP information comes from a trusted source, the video conferencing device must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 10)

The ID, which is part of the ID/key pair that the NTP source uses.

## NetworkServices NTP Server [n] KeyAlgorithm

n: 1..3

Choose the authentication hash function that the NTP server uses, and that the video conferencing device must use to authenticate the time messages.

Requires user role: ADMIN

Default value: ""

Value space: None/SHA1/SHA256

None: The NTP server doesn't use a hash function.

SHA1: The NTP server uses the SHA-1 hash function.

SHA256: The NTP server uses the SHA-256 hash function (from the SHA-2 family of hash functions).

## NetworkServices SIP Mode

Define whether the device 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.

## NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used by network management systems to monitor and manage devices such as routers, servers, and switches, that are connected to the IP network. SNMP exposes management data in the form of variables on the managed devices, which describe the device status and configuration. These variables can then be remotely queried, and sometimes set, by managing applications.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

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 [n] Address

n: 1..3

Not applicable in this version.

Requires user role: ADMIN, INTEGRATOR

## NetworkServices SNMP CommunityName

Define the name of the SNMP community. The SNMP community name is used to authenticate SNMP requests. If an SNMP request from a management system does not include a matching community name (case sensitive), the message is dropped and the SNMP agent in the video device will not send a response.

If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP community is configured there.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

The SNMP community name.

## NetworkServices SNMP SystemContact

Define contact information that SNMP servers can use.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

String that describes the contact information for the video device.

## NetworkServices SNMP SystemLocation

Define location information that SNMP servers can use.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

String that describes the location of the video device.

## NetworkServices SSH Mode

The SSH (or Secure Shell) protocol can provide secure encrypted communication between the video conferencing device 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 HostKeyAlgorithm

Choose the cryptographic algorithm that shall be used for the SSH host key. Choices are RSA (Rivest-Shamir-Adleman) with 2048 bits keysize, ECDSA (Elliptic Curve Digital Signature Algorithm) with NIST curve P-384, and EdDSA (Edwards-curve Digital Signature Algorithm) with ed25519 signature schema.

Requires user role: ADMIN

Default value: RSA

Value space: ECDSA/RSA/ed25519

ECDSA: Use the ECDSA algorithm (nist-384p).

RSA: Use the RSA algorithm (2048 bits).

ed25519: Use the ed25519 algorithm.

## NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the device.

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 UPnP Mode

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video conferencing device has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video conferencing device. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting.

When UPnP is enabled, the device advertises its presence on the network. The advertisement permits a Touch controller to discover video conferencing devices automatically, and you do not need to manually enter the device'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 conferencing device does not advertise its presence, and you have to enter the device's IP address manually in order to pair a Touch controller to the device.

On: UPnP is enabled. The video conferencing device advertises its presence until the timeout period expires.

## NetworkServices UPnP Timeout

Define for how many seconds UPnP shall stay enabled after the device 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: Integer (0..3600)

Range: Select a value between 0 and 3600 seconds.

## NetworkServices Websocket

It is possible to interact with the API of the device over the WebSocket protocol, both the insecure and secure versions (ws and wss). A WebSocket is tied to HTTP, so that also HTTP or HTTPS must be enabled before you can use WebSockets (see the NetworkServices HTTP Mode setting).

Requires user role: ADMIN

Default value: Off

Value space: FollowHTTPService/Off

FollowHTTPService: Communication over the WebSocket protocol is allowed when HTTP or HTTPS is enabled.

Off: Communication over the WebSocket protocol is not allowed.

## NetworkServices WelcomeText

Choose which information the user should see when logging on to the device through 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 Wifi Allowed

Devices that have a built-in Wi-Fi adapter, can connect to the network either via Ethernet or Wi-Fi. Both Ethernet and Wi-Fi are allowed by default, and the user can choose which one to use from the user interface. With this setting, the administrator can disable Wi-Fi configuration, so that it cannot be set up from the user interface.

The devices support the following standards: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac. The device supports the following security protocols: WPA-PSK (AES), WPA2-PSK (AES), EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, EAP-MSCHAPv2, EAP-GTC, and open networks (not secured).

If the PID (Product ID), found on the rating label at the rear of the device, contains the letters NR (No Radio) the device does not support Wi-Fi.

Requires user role: ADMIN, USER

Default value: True

Value space: False/True

False: Wi-Fi cannot be used. You must connect to the network via Ethernet.

True: Both Ethernet and Wi-Fi are allowed.

## NetworkServices Wifi Enabled

Provided that the device is allowed to connect to the network via Wi-Fi (see the NetworkServices WIFI Allowed setting), you can use this setting to enable and disable Wi-Fi.

You cannot use Ethernet and Wi-Fi at the same time. If you try to configure Wi-Fi while an Ethernet cable is connected, you must unplug the Ethernet cable to proceed. If you connect an Ethernet cable while connected to Wi-Fi, Ethernet will take precedence. If you unplug the Ethernet cable, the device will automatically connect to the last connected Wi-Fi network, if available.

Requires user role: ADMIN, USER

Default value: True

Value space: False/True

False: Wi-Fi is disabled.

True: Wi-Fi is enabled.

## NetworkServices XMLAPI Mode

Enable or disable the device'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 device.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The XML API is disabled.

On: The XML API is enabled.

## Peripherals settings

### Peripherals InputDevice Mode

Define whether or not to allow the use of a third-party input device, such as a USB keyboard or a wireless remote control with a USB dongle. The input device must advertise itself as a USB keyboard. You must define and implement the actions to be taken as response to key clicks yourself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: A third-party USB input device is not allowed.

On: A third-party USB input device can be used to control certain functions on the video conferencing device.

### Peripherals Pairing CiscoTouchPanels EmcResilience

If the Touch controller is used in environments with considerable amounts of electromagnetic noise present, you may experience an appearance of false signals—for example as if someone tapped the Touch controller when obviously nobody did so. To cope with this you may enable the EMC Resilience Mode.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The EMC resilience is disabled.

On: The EMC resilience is enabled.

### Peripherals Pairing CiscoTouchPanels RemotePairing

In order to use Cisco Touch 10 (touch panel) as user interface for the video conferencing device, Touch 10 must be either directly connected to the device or paired to the device via LAN. The latter is referred to as remote pairing.

Remote pairing is allowed by default; you must switch this setting Off if you want to prevent remote pairing.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Remote pairing of Touch 10 is not allowed.

On: Remote pairing of Touch 10 is allowed.

### Peripherals Profile Cameras

Define the number of cameras that are expected to be connected to the video conferencing device. This information is used by the device'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, INTEGRATOR

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 device.

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

## Peripherals Profile ControlSystems

Define if a third-party control system, for example Crestron or AMX, is expected to be connected to the video conferencing device. This information is used by the video conferencing device'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 conferencing device using xCommand Peripherals Pair and HeartBeat commands. Failing to do so will cause the video conferencing device to show a warning that it has lost connectivity to the control system.

Requires user role: ADMIN, INTEGRATOR

Default value: NotSet

Value space: 1/NotSet

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

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

## Peripherals Profile TouchPanels

Define the number of Cisco Touch controllers that are expected to be connected to the device. This information is used by the device's diagnostics service. If the number of connected Touch controllers does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN, INTEGRATOR

Default value: Minimum1

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

NotSet: No touch panel check is performed.

Minimum1: At least one Cisco Touch controller should be connected to the device.

0-5: Select the number of Touch controllers that are expected to be connected to the device. Note that only one Cisco Touch controller is officially supported.

## Phonebook settings

### Phonebook Server [n] ID

n: 1..1

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 [n] Pagination

n: 1..1

Configure if the phonebook server supports pagination (paging) or not. Pagination means that the server supports consecutive searches, and these searches can be relative to an offset. This allows the user interface to perform as many consecutive searches as required to get the complete search result.

If Pagination is Disabled the device does a single search and returns a maximum of 100 entries in the search result. It is not possible to scroll to any further search results beyond that.

Requires user role: ADMIN

Default value: Enabled

Value space: Disabled/Enabled

Disabled: The phonebook server does not support pagination. The device does a single search, and the maximum number of entries in the search result is 100.

Enabled: The phonebook server supports pagination.

### Phonebook Server [n] TlsVerify

This setting applies when a video conferencing device connects to an external phone book server via HTTPS.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.



## Phonebook Server [n] Type

n: 1..1

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 in the Cisco Webex cloud service.

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 [n] URL

n: 1..1

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 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 device 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 device 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 device will be provisioned by the alternate CUCM. When the main CUCM is available again, the device 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 selected 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.

## Provisioning Mode

It is possible to configure a device using a provisioning system (external manager). This allows video conferencing network administrators to manage many devices 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/Webex/TMS/VCS

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

Auto: The provisioning server is automatically selected as set up in the DHCP server.

CUCM: Push configurations to the device from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the device from CUCM (Cisco Unified Communications Manager). The device connects to CUCM via the Expressway infrastructure. In order to register over Expressway the encryption option key must be installed on the device.

Webex: Push configurations to the device from the Cisco Webex cloud service.

TMS: Push configurations to the device from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the device from VCS (Cisco TelePresence Video Communication Server).

## Provisioning LoginName

This is the username part of the credentials used to authenticate the device 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 device 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 TlsVerify

This setting applies when a video conferencing device connects to a provisioning server via HTTPS.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

The certificate check is always performed, regardless of this setting, if the device is provisioned from the Cisco Webex cloud service or from CUCM via Expressway (also known as MRA or Edge).

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.

## Provisioning WebexEdge

Define if the device is linked to Webex Edge for Devices, which gives access to select Webex cloud services.

The setting applies only to devices that are registered to an on-premises service.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: The device is not linked to Webex Edge for Devices.

On: The device is linked to Webex Edge for Devices.

## Proximity settings

### Proximity AlternatePort Enabled

This setting applies only when NetworkServices HTTP Mode is set to HTTP+HTTPS or HTTPS.

By default, Proximity connections use TCP port 443. Use this setting to allow Proximity connections also on port 65533.

Requires user role: ADMIN

Default value: False

Value space: False/True

False: Proximity connections always use TCP port 443.

True: Proximity connections can use either TCP port 443 or 65533. The port used depends on the client.

### Proximity Mode

The Proximity Mode setting has no effect for devices that are registered to the Webex cloud service. To prevent a cloud registered device from sending ultrasound pairing messages, you must set Audio Ultrasound MaxVolume to 0.

For devices registered on-premises, the Proximity Mode setting determines whether the device will emit ultrasound pairing messages or not. When the device emits ultrasound pairing messages, Cisco collaboration clients can detect that they are close to the device.

In order to use a client, at least one of the Proximity services must be enabled (refer to the Proximity Services settings) as well. In general, Cisco recommends enabling all the Proximity services.

The Proximity Mode and Audio Ultrasound MaxVolume settings only affect ultrasound pairing messages. To stop all ultrasound emissions, the RoomAnalytics PeoplePresenceDetector and Standby WakeupOnMotionDetection settings must also be switched Off.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: Cisco collaboration clients cannot detect that they are close to the device, thus Proximity services cannot be used.

On: Cisco collaboration clients can detect that they are close to the device, and enabled Proximity services can be used.

### Proximity Services CallControl

Enable or disable basic call control features on Cisco collaboration clients. When this setting is enabled, you are able to control a call using a Cisco collaboration 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 Cisco collaboration client is enabled.

Disabled: Call control from a Cisco collaboration client is disabled.

## Proximity Services ContentShare FromClients

Enable or disable content sharing from Cisco collaboration clients. When this setting is enabled, you can share content from a Cisco collaboration client wirelessly on the device, 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 Cisco collaboration client is enabled.

Disabled: Content sharing from a Cisco collaboration client is disabled.

## Proximity Services ContentShare ToClients

Enable or disable content sharing to Cisco collaboration clients. When enabled, Cisco collaboration clients will receive the presentation from the device. 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 Cisco collaboration client is enabled.

Disabled: Content sharing to a Cisco collaboration client is disabled.

## RoomAnalytics settings

### RoomAnalytics AmbientNoiseEstimation Mode

The device can estimate the stationary ambient noise level (background noise level) in the room. The result is reported in the RoomAnalytics AmbientNoise Level dBA status. The status is updated when a new ambient noise level is detected.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

On: The device regularly estimates the stationary ambient noise level.

Off: The device doesn't estimate the stationary ambient noise level.

### RoomAnalytics PeopleCountOutOfCall

By using face detection, the device – when a Cisco Quad Camera is connected – has the capability to find how many persons are in the room. By default, the device only counts people when in a call, or when displaying the self-view picture.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

Off: The device counts people only when the device is in a call, or when self-view is on.

On: The device counts people as long as the device is not in standby mode. This includes outside of call, even if self-view is off.

### RoomAnalytics PeoplePresenceDetector

The device has the capability to find whether or not people are present in the room, and report the result in the RoomAnalytics PeoplePresence status. The feature is based on ultrasound. Read the status description for more details.

Ultrasound signals for presence detection are not emitted when both this setting AND the Standby WakeupOnMotionDetection setting are switched Off. The Audio Ultrasound MaxVolume and Proximity Mode settings has no effect on presence detection.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

Off: Information about the presence of people is not reported in the device's status.

On: Information about the presence of people is reported in the device's status.

## RoomReset settings

### RoomReset Control

This setting is for use with control systems or macros. Macros allow you to write snippets of JavaScript code that can automate parts of your video conferencing device, thus creating custom behavior.

When a room has been idle for some time the video conferencing device can send an event to indicate that the room is ready to be reset.

The events that are sent when this setting is enabled are:

```
*e RoomReset SecondsToReset: 30
```

```
** end
```

```
*e RoomReset Reset
```

```
** end
```

Requires user role: ADMIN

Default value: On

Value space: CameraPositionsOnly/Off/On

CameraPositionsOnly: Not applicable.

Off: No RoomReset events will be sent.

On: The room reset control is enabled and RoomReset events will be sent.



## RTP settings

### RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the device is using the ports in the range 2326 to 2487 for RTP and RTCP media data. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2326

Value space: Integer (1024..65438)

Set the first port in the range of RTP ports. The value must be an even number.

### RTP Ports Range Stop

Define the last port in the range of RTP ports.

As default, the device is using the ports in the range 2326 to 2487 for RTP and RTCP media data. If the RTP Video Ports Range is enabled the device is using the ports in the range 1024 to 65436. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2487

Value space: Integer (1121..65535)

Set the last port in the range of RTP ports. The value must be an odd number. If you enter an even value, +1 will be automatically applied.

### RTP Video Ports Range Start

Define the first port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65454)

Set the first port in the range of RTP video ports.

### RTP Video Ports Range Stop

Define the last port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65535)

Set the last port in the range of RTP video 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. This setting has no effect if the Logging Mode setting is set to Off.

When using the External or ExternalSecure mode you must enter the address of the audit server in the Security Audit Server Address setting.

Requires user role: AUDIT

Default value: Internal

Value space: External/ExternalSecure/Internal/Off

**External:** The device sends the audit logs to an external syslog server. The syslog server must support UDP.

**ExternalSecure:** The device 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 device using the web interface. The `common_name` parameter of a certificate in the CA list must match the IP address or DNS name of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

**Internal:** The device records the audit logs to internal logs, and rotates logs when they are full.

**Off:** No audit logging is performed.

### 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 device 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 device 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

Set the IP address or DNS name of the syslog server that the audit logs are sent to. 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, IPv6 address, or DNS name.

### Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the device 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 Setup > 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 Fips Mode

If required, you can set the device in FIPS mode (Federal Information Processing Standard (FIPS) Publication 140-3, Security Requirements for Cryptographic Modules). While in FIPS mode the remote support user is not available, and Digest access authentication is not supported between the device and an HTTP Proxy, because Digest access authentication is using MD5 cryptographic hashing, which is not allowed in FIPS. This last limitation only affects Webex registered devices, since an HTTP Proxy is used only for the Webex solution.

You should allow only HTTPS, and do not switch on SNMP or IEEE8021X in FIPS mode (keep the default values).

For changes to this setting to take full effect, you must restart the device.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The device is not in FIPS mode.

On: The device is in FIPS mode.

## Security Session FailedLoginsLockoutTime

Define how long the device will lock out a user after failed login to a web or SSH session. Restart the device for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 60

Value space: Integer (0..10000)

Set the lockout time (minutes).

## Security Session InactivityTimeout

Define how long the device will accept inactivity from the user before he is automatically logged out from a web or SSH session.

Restart the device 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 MaxFailedLogins

Define the maximum number of failed login attempts per user for a web or SSH session. If the user exceeded the maximum number of attempts the user will be locked out. 0 means that there is no limit for failed logins.

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10)

Set the maximum number of failed login attempts per user.

## Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions per user.

## Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions in total.

## Security Session ShowLastLogon

When logging in to the device using SSH 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.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the serial port.

On: Enable the serial port.

### SerialPort BaudRate

Set the baud rate (data transmission rate, bits per second) for the serial port.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

Requires user role: ADMIN, INTEGRATOR

Default value: 115200

Value space: 115200

Choose a baud rate from the baud rates listed (bps).

### SerialPort LoginRequired

Define if login shall be required when connecting to the serial port.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The user can access the device via the serial port without any login.

On: Login is required when connecting to the device 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 username 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: Auto/TCP/Tls/UDP

TCP: The device will always use TCP as the default transport method.

UDP: The device will always use UDP as the default transport method.

Tls: The device will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the device. If no such CA-list is available on the device then anonymous Diffie Hellman will be used.

Auto: The device 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 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 device 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 device's private IP address.

Rflx: Send media to the device'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 Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the devices can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the devices. Initially STUN (Session Traversal Utilities for NAT) messages are exchanged when setting up the media path.

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 Line

When registered to a Cisco Unified Communications Manager (CUCM) the device 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 device. Therefore do not change this setting manually; CUCM pushes this information to the device when required.

Requires user role: ADMIN

Default value: Private

Value space: Private/Shared

Shared: The device is part of a shared line and is therefore sharing its directory number with other devices.

Private: This device is not part of a shared line.

## SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the device will only be reachable through a SIP Proxy (CUCM or VCS). As a security measure, SIP ListenPort should be Off when the device is registered to a SIP Proxy.

Requires user role: ADMIN

Default value: On

Value space: Auto/Off/On

Auto: Listening for incoming connections on the SIP TCP/UDP ports is automatically turned off if the device is registered to a SIP Proxy; otherwise it is turned 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 MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.0

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.

## 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 [n] Address

n: 1..4

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

Before establishing a connection over SIP TLS, the device checks if the certificate of the peer is signed by a trusted Certificate Authority (CA). The CA must be included in the CA list that is manually uploaded to the device using the web interface or API. The list of pre-installed certificates is not used to validate certificates for SIP TLS connections.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the setting was not explicitly set to On.

Use the SIP MinimumTLSVersion setting to specify which TLS versions are allowed.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The device doesn't check the certificate of the peer. The SIP TLS connection is established anyway.

On: The device checks if the certificate of the peer can be trusted. If not, the SIP TLS connection is not established.



## SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the device 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 device will search for available Turn servers in DNS, and before making calls the device will test if port allocation is possible.

## SIP Turn DropRflx

DropRflx will make the device force media through the Turn relay, unless the remote device is on the same network.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable DropRflx.

On: The device will force media through the Turn relay when the remote device 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 device'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 username needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid username.

## 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).

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 device. The URI is registered and used by the SIP services to route inbound calls to the device. 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 BootAction

Define the camera position after a restart of the video conferencing device.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: DefaultCameraPosition

Value space: None/DefaultCameraPosition/RestoreCameraPosition

None: No action.

RestoreCameraPosition: When the video conferencing device restarts, the camera returns to the position that it had before the restart.

DefaultCameraPosition: When the video conferencing device restarts, the camera moves to the factory default position.

### Standby Control

Define whether the device should go into standby mode or not.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The device will not enter standby mode.

On: The device will enter standby mode when the Standby Delay has timed out.

### Standby Delay

Define how long (in minutes) the device shall be in idle mode before it goes into standby mode. Requires the Standby Control to be enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..480)

Set the standby delay (minutes).

### Standby Signage Audio

By default, a device does not play out audio in digital signage mode even if the web page has audio. You can use this setting to override the default behavior.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: The device does not play out audio with the web page.

On: If the web page has audio, the device plays it out. The volume follows the volume setting of the device.

### Standby Signage Mode

Content from a URL (a web page) can replace the traditional half-wake background image and information. This feature is called digital signage.

The use of digital signage does not prevent the device from entering standby the normal way. Therefore, the Standby Delay setting determines for how long the digital signage is shown before the device goes into standby.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Digital signage is not enabled on the device.

On: Digital signage is enabled and replaces the device's half-wake mode, provided that also the WebEngine Mode setting is On.

## Standby Signage RefreshInterval

You can use this setting to force a web page to refresh at regular intervals. This is useful for web pages that are not able to refresh themselves. It is not recommended to set a refresh interval with the interactive mode.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (0..1440)

The number of seconds between each web page refresh. The value of 0 means that the web page is never forced to refresh.

## Standby Signage Url

Set the URL of the web page you want to display on the screen (digital signage). If the length of the URL is 0, the device retains normal half-wake mode. If the URL fails, the device retains normal half-wake mode and a diagnostics message is issued.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 2000)

The URL of the web page.

## Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN, INTEGRATOR

Default value: PrivacyPosition

Value space: None/PrivacyPosition

None: No action.

PrivacyPosition: When the video conferencing device 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, INTEGRATOR, USER

Default value: RestoreCameraPosition

Value space: None/RestoreCameraPosition/DefaultCameraPosition

None: No action.

RestoreCameraPosition: When the video conferencing device leaves standby, the camera returns to the position that it had before entering standby.

DefaultCameraPosition: When the video conferencing device leaves standby, the camera moves to the factory default position.

## Standby WakeupOnMotionDetection

Automatic wake up on motion detection is a feature that allows the device to detect when people enter the room. The feature is based on ultrasound detection.

Ultrasound signals for motion detection are not emitted when both this setting AND the RoomAnalytics PeoplePresenceDetector setting are switched Off. The Audio Ultrasound MaxVolume and Proximity Mode settings has no effect on motion detection.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Wake up on motion detection is disabled.

On: When people walk into the room the device will automatically wake up from standby.

## SystemUnit settings

### SystemUnit Name

Define the device name. The device name will be sent as the hostname in a DHCP request and when the device is acting as an SNMP Agent.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

Define the device name.

### SystemUnit CrashReporting Advanced

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The ACR tool will perform standard log analyses.

On: The ACR tool will perform advanced log analyses.

### SystemUnit CrashReporting Mode

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: No logs will be sent to ACR tool.

On: The logs will automatically be sent to ACR tool.

### SystemUnit CrashReporting Url

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: "acr.cisco.com"

Value space: String (0..255)

The URL to the Cisco Automatic Crash Report tool (ACR).

## 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 device. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: ADMIN, INTEGRATOR, 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/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New\_York, America/Nipigon, America/Nome, America/Noronha, America/North\_Dakota/Beulah, America/North\_Dakota/Center, America/North\_Dakota/New\_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port\_of\_Spain, America/Porto\_Acre, America/Porto\_Velho, America/Puerto\_Rico, America/Rainy\_River, America/Rankin\_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio\_Branco, America/Rosario, America/Santa\_Isabel, America/Santarem, America/Santiago, America/Santo\_Domingo, America/Sao\_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St\_Barthelemy, America/St\_Johns, America/St\_Kitts, America/St\_Lucia, America/St\_Thomas, America/St\_Vincent, America/Swift\_Current, America/Tegucigalpa, America/Thule, America/Thunder\_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South\_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/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/Te\_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 Accessibility IncomingCallNotification

You can enable an incoming call notification with amplified visuals. The screen and Touch 10 will flash red/white approximately once every second (1.75 Hz) to make it easier for hearing impaired users to notice an incoming call. If the device is already in a call the screen will not flash as this will disturb the on-going call, instead you will get a normal notification on screen and touch panel.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Default

Value space: AmplifiedVisuals/Default

AmplifiedVisuals: Enable the amplified visuals on screen and touch panel when the device receives a call.

Default: Enable the default behavior with a notification on screen and touch panel.

### UserInterface Assistant Mode

Webex Assistant allows you to control the device by using voice commands. Webex Assistant is a cloud service, so the device must either be registered to the Webex cloud service or registered to an on-premises service and linked to Webex Edge for Devices.

Use this setting to enable or disable the Webex Assistant on the device.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Webex Assistant is switched off.

On: Webex Assistant can be used if it is supported by the infrastructure.

### UserInterface Assistant Mode

Proactive Join is a feature that is offered by Webex Assistant. When Proactive Join is enabled and someone is discovered in the meeting room just before the start of an OBTP-meeting, the device will ask if they want to join the meeting that is about to start.

Use this setting to enable or disable the Proactive Join feature on the device.

Requires user role: ADMIN

Default value: False

Value space: False/True

False: The Proactive Join feature is switched off.

True: The Proactive Join feature can be used if Webex Assistant is active.

### UserInterface Branding AwakeBranding Colors

If the device is set up with branding customizations, this setting affects the colors of the logo that is shown when the device is awake. You can choose whether you want to show the logo in full color, or reduce the opacity of the logo so that it blends in more naturally with the background and other elements on the screen.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Native

Auto: The opacity of the logo is reduced.

Native: The logo has full colors.

## UserInterface ContactInfo Type

Choose which type of contact information to show in the user interface.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/SystemName

Auto: Show the address which another device should dial to reach this video conferencing device. The address depends on the default call protocol and device registration.

None: Do not show any contact information.

IPv4: Show the device's IPv4 address.

IPv6: Show the device's IPv6 address.

H323Id: Show the device's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the device's H.320 number as contact information (only supported if used with Cisco TelePresence ISDN Link).

E164Alias: Show the device's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

SipUri: Show the device's SIP URI (refer to the SIP URI setting).

SystemName: Show the device's name (refer to the SystemUnit Name setting).

DisplayName: Show the device's display name (refer to the SIP DisplayName setting).

## UserInterface CustomMessage

A custom message can be displayed, in the lower left side of the screen, in awake mode.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 128)

Add a custom message. Add an empty string to remove a custom message.

## UserInterface KeyTones Mode

You can configure the device to make a keyboard click sound effect (key tone) when typing text or numbers.

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 Features Call End

Choose whether or not to remove the default End Call button from the user interface. The setting removes only the button, not its functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

## UserInterface Features Call MidCallControls

Choose whether or not to remove the default Hold, Transfer, and Resume in-call buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

## UserInterface Features Call JoinWebex

Choose whether or not to remove the default Join Webex button from the user interface. The button allows users to dial into a Webex meeting using just the Webex meeting number, no domain is required. However, for this to work, you must set up the infrastructure to allow calls to be routed to \*@webex.com.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

## UserInterface Features Call Start

Choose whether or not to remove the default Call button (including the directory, favorites, and recent calls lists) and the default in-call Add participant button from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

## UserInterface Features Call VideoMute

Choose whether or not to show the default "Turn video off" button in the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the "Turn video off" button in the user interface if this feature is supported in the ongoing call.

Hidden: The "Turn video off" button is never shown in the user interface.

## UserInterface Features HideAll

Choose whether or not to remove all default buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: False

Value space: False/True

False: Shows all default buttons in the user interface.

True: Removes all default buttons from the user interface.

## UserInterface Features Share Start

Choose whether or not to remove the default buttons and other UI elements for sharing and previewing content, both in call and out of call, from the user interface. The setting removes only the buttons and UI elements, not their functionality as such. You can share content using Proximity or the Cisco Webex Teams app still.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons and UI elements in the user interface.

Hidden: Removes the default buttons and UI elements from the user interface.

## UserInterface Language

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

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/Portuguese/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish

Select a language from the list.

## UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a 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. Then, an encryption indicator icon is shown for the rest of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. No encryption indicator icon is shown.

AlwaysOn: The "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

AlwaysOff: The encryption indicator is never displayed on screen.

## UserInterface OSD HalfwakeMessage

A custom message can be displayed in the middle of the main screen when the device is in the half wake state. The custom message will replace the default message, which gives instructions how to start using the device. You can also delete the default message, without adding a custom message.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

The custom message. An empty string: Restore the default message. A space only: There will be no message at all.

## UserInterface OSD Output

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/1/2

Auto: The device detects when a monitor is connected to a video output, and sends the on-screen information and indicators to the first monitor you connect. If you have a multi-monitor setup, and all monitors are connected before switching on the device, the on-screen information and indicators are sent to the video output with the lowest number, starting with Output Connector 1 (HDMI 1).

1-2: The device sends the on-screen information and indicators to the specified output. Choose n to send the on-screen information and indicators to the device's Output Connector n.

## UserInterface Phonebook Mode

This setting determines if a user is allowed to add or change a contact in the Directory and Favorites list from the user interface of the device.

Requires user role: ADMIN, INTEGRATOR

Default value: ReadWrite

Value space: ReadOnly/ReadWrite

ReadOnly: You neither can add a contact to the Favorites list, edit a contact in the Favorites list, nor edit any contact from the Directory or Favorites list before calling.

ReadWrite: You are able to add a contact to the Favorites list, edit a contact in the Favorites list, and edit a contact from the Directory or Favorites list before calling.

## UserInterface Security Mode

This setting allows you to prevent important device information from being exposed in the user interface (drop down menu and Settings panel), for example the contact information and IP addresses of the video conferencing device, touch controller, and UCM/VCS registrars. It is important to note that such information is not hidden when navigating further into the Settings panel.

If you want to fully prevent that people without administrator rights can see the contact information, IP addresses, MAC address, serial number, and software version, you must also set the UserInterface SettingsMenu Mode to Locked, and of course have a passphrase for all user accounts with administrator rights.

Requires user role: ADMIN

Default value: Normal

Value space: Normal/Strong

Normal: IP addresses and other device information are shown on the user interface.

Strong: Contact information and IP addresses are not displayed on the user interface (drop down menu and Settings panel).

## UserInterface SettingsMenu Mode

The Settings panel in the user interface (Touch 10 or on-screen) can be protected by the device's admin password. If this password is blank, anyone can access the settings in the Settings panel, and for example factory reset the device. If authentication is enabled, all settings that require authentication have a padlock icon. You will be prompted to enter the administrator's username and passphrase when you select the setting. Some settings do not require authentication, they do not have a padlock icon.

Requires user role: ADMIN

Default value: Unlocked

Value space: Locked/Unlocked

Locked: Authentication with administrator's username and passphrase is required.

Unlocked: No authentication is required.

## UserInterface SettingsMenu Visibility

Choose whether or not to show the device name (or contact information) and the associated drop down menu and Settings panel on the user interface.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the device name with drop down menu and Settings panel on the user interface.

Hidden: Doesn't show the device name with drop down menu and Settings panel on the user interface.

## UserInterface SoundEffects Mode

You can configure the device to make a sound effect, e.g. when someone connects a laptop or mobile through Proximity.

The keyboard click sound effect when typing text is not affected by this setting (refer to the UserInterface Keytones Mode setting).

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: There are no sound effects.

On: The sound effects are switched on.

## UserInterface Wallpaper

Select a background image (wallpaper) for the video screen when idle.

You may upload a custom wallpaper to the device 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, INTEGRATOR, 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 device, the setting will revert to the default value.

## UserManagement settings

### UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges.

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

Refer to the LDAP specification for the syntax of this string. Example:

```
"(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)
(sAMAccountName=username))"
```

### 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>).

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

The distinguished 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.

### UserManagement LDAP BaseDN

The distinguishing name of the entry at which to start a search (base).

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

The distinguishing name of the base. Example: "DC=company, DC=com"

### UserManagement LDAP Encryption

Define how to secure the communication between the device 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 the LDAP server on port 389 with no encryption.

STARTTLS: Connect to the LDAP server on port 389, then send a STARTTLS command to upgrade to an encrypted connection (TLS).

## 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 Mode

The device supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate usernames 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.

If you switch on LDAP Mode, make sure to configure the other UserManagement LDAP settings to suit your setup. Here is a few examples.

Example 1:

- UserManagement LDAP Mode: On
- UserManagement LDAP Address: "192.0.2.20"
- UserManagement LDAP BaseDN: "DC=company, DC=com"
- UserManagement LDAP Admin Group: "CN=admin group, OU=company groups, DC=company, DC=com"

Example 2:

- UserManagement LDAP Mode: On
- UserManagement LDAP Address: "192.0.2.20"
- UserManagement LDAP BaseDN: "DC=company, DC=com"
- UserManagement LDAP Admin Filter: "(!(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: LDAP authentication is not allowed.

On: LDAP authentication is allowed.

## 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 VerifyServerCertificate

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

On: The device 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 device in advance. Use the device's web interface to manage the list of trusted CAs (see more details in the administrator guide).



## UserManagement PasswordPolicy Complexity MinimumDigits

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the “systemtools securitysetting” command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of numerical characters (0..9) in the password.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..4)

The minimum number of numerical characters. 0 means no restrictions.

## UserManagement PasswordPolicy Complexity MinimumLength

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the “systemtools securitysetting” command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of characters in the password.

Requires user role: ADMIN

Default value: 8

Value space: Integer (0..256)

The minimum number of characters. 0 means no restrictions.

## UserManagement PasswordPolicy Complexity MinimumLowercase

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the “systemtools securitysetting” command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of lower-case letters in the password.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..4)

The minimum number of lower-case characters. 0 means no restrictions.

## UserManagement PasswordPolicy Complexity MinimumSpecial

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the “systemtools securitysetting” command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of special characters in the password.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..4)

The minimum number of special characters. 0 means no restrictions.

## UserManagement PasswordPolicy Complexity MinimumUppercase

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the "systemtools securitysetting" command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of upper-case letters in the password.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..4)

The minimum number of upper-case characters. 0 means no restrictions.

## UserManagement PasswordPolicy MaxLifetime

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the "systemtools securitysetting" command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the maximum number of days before a password becomes invalid.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..7300)

The minimum number of days. 0 means no restrictions.

## UserManagement PasswordPolicy ReuseLimit

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. These settings replace the "systemtools securitysetting" command that was available in software versions older than CE9.10.

A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the reuse limit (n), which means that a user cannot change to either of their previous n passwords.

Requires user role: ADMIN

Default value: 12

Value space: Integer (0..24)

The minimum number of passwords. 0 means no restrictions.

## 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, INTEGRATOR

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 device, 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 in the stream that is sent to the remote participants (far end). This setting applies only when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

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 to be used as the default main video source when you start a call.

Requires user role: ADMIN, USER

Default value: 1

Value space: 1/2/3

The source that is used as the default main video source.

## Video Input Connector [n] CameraControl Camerald

n: 1..3

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: n

Value space: Connector n: 1/2/3/4/5/6/7

Select the ID of the camera.

## Video Input Connector [n] CameraControl Mode

n: 1..3

Define whether the camera that is connected to this video input connector can be controlled or not.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: On

Value space: Connector n: Off/On

Off: Disable camera control.

On: Enable camera control.

## Video Input Connector [n] CEC Mode

n: 1..3

The video input (HDMI) supports Consumer Electronics Control (CEC). When this setting is enabled, information about the connected device (for example device type and device name) is available in the video conferencing device status (Video Input Connector[n] ConnectedDevice CEC [n]), provided that the connected device also supports CEC.

If you have Cisco Quad Camera, do not switch off CEC on that connector because then there will be no sound on the speakers on the camera. CEC is required for HDMI ARC (Audio Return Channel), which is the channel used for sending audio from the video conferencing device to the camera.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Connector n: Off/On

Off: CEC is disabled.

On: CEC is enabled.

## Video Input Connector [n] HDCP Mode

n: 1..3

One of the video conferencing device's HDMI inputs can be configured to support HDCP protected content (High-bandwidth Digital Content Protection, version 1.4). This allows customers to re-purpose a video conferencing device's screen by connecting devices such as a Google ChromeCast, an AppleTV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the input connector is configured to support HDCP, it is reserved for this type of content. This means that you can't share any content from this specific connector while in a call, regardless of what is connected, nor can you take web snapshots of this source.

HDCP protected content is displayed on the screen that is connected to output connector 1. The screen must support HDCP.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

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

Off: Disable support for HDCP protected content on this video input connector.

On: Enable support for HDCP protected content this video input connector.

## Video Input Connector [n] InputSourceType

n: 1..3

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: camera Other connectors: PC

Value space: Connector n: PC/camera/document\_camera/mediaplayer/whiteboard/other

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

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

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.

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 [n] Name

n: 1..3

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: "Camera" Connector 2: "PC 1 (HDMI)" Connector 3: "PC 2 (HDMI)"

Value space: String (0, 50)

Name for the video input connector.

## Video Input Connector [n] OptimalDefinition Profile

n: 1..3

This setting will not take effect if the corresponding Video Input Connector [n] Quality setting is set to Sharpness.

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. 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 devices.

Requires user role: ADMIN, INTEGRATOR

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 [n] OptimalDefinition Threshold60fps

n: 1..3

For each video input, this setting tells the device the lowest resolution where it can transmit 60 fps. So for all resolutions lower than this, the maximum transmitted frame rate would be 30 fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Requires user role: ADMIN

Default value: 1920\_1080

Value space: 512\_288/768\_448/1024\_576/1280\_720/1920\_1080/Never

512\_288: Set the threshold to 512x288.

768\_448: Set the threshold to 768x448.

1024\_576: Set the threshold to 1024x576.

1280\_720: Set the threshold to 1280x720.

1920\_1080: Set the threshold to 1920x1080.

Never: Do not set a threshold for transmitting 60fps.

## Video Input Connector [n] PreferredResolution

n: 1..3

Define the preferred screen resolution and refresh rate that the video conferencing device advertises to the input sources that are connected via HDMI (for example a laptop). The logic for selection of the resolution on the source side will choose this resolution and refresh rate automatically, unless it is overridden manually by the source device (for example the laptop's display configuration software).

Note that the formats 2560\_1440\_60 and 3840\_2160\_30 use about twice the amount of data compared to the 1920\_1080\_60 format, and requires a presentation cable (or adapter) that is qualified for at least HDMI 1.4b data rates.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: 1920\_1080\_60

Value space: Connector 1: 1920\_1080\_60 Connector 2,3 : 1920\_1080\_60/2560\_1440\_60/3840\_2160\_30

1920\_1080\_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

2560\_1440\_60: The resolution is 2560 x 1440, and the refresh rate is 60 Hz.

3840\_2160\_30: The resolution is 3840 x 2160, and the refresh rate is 30 Hz.

## Video Input Connector [n] PresentationSelection

n: 1..3

Define how the video conferencing device will behave when you connect a presentation source to the video input. In general, any input source can be used as a presentation source; normally, the main camera will not be used as a presentation source.

If the device 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, INTEGRATOR

Default value: Connector 1: Manual Other connectors: OnConnect

Value space: Connector n: 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 [n] Quality

n: 1..3

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.

If a Quad Camera or a Precision 60 camera is detected by the device this setting is automatically set to Motion. If a user changes this setting manually, it will be set back to Motion after a restart or a camera reconnect.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Motion Connector 2,3: Sharpness

Value space: Connector n: 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 [n] RGBQuantizationRange

n: 1..3

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, INTEGRATOR

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 [n] Visibility

n: 1..3

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Never Other connectors: Always

Value space: Connector n: Always/IfSignal/Never

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: The menu selection for the video input connector will only be visible when something is connected to the video input.

Never: The input source is not expected to be used as a presentation source, and will not show up on the user interface.

## Video Monitors

A monitor role is assigned to each screen using the Video Output Connector [n] MonitorRole setting. The monitor role decides which layout (call participants and presentation) will appear on the screen that is connected to this output. Screens with the same monitor role will get the same layout; screens with different monitor roles will have different layouts.

The monitor layout mode that is set in the Video Monitors setting should reflect the number of different layouts you want in your room setup. Note that some screens can be reserved for presentations.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Single/Dual/DualPresentationOnly

Auto: The number of screens connected to the device is automatically detected, and the layout is distributed on the screens according to the monitor role.

Single: The same layout is shown on all screens.

Dual: The layout is distributed on screens with monitor role First and Second. If a presentation is part of the layout, all participants in the call are shown on the screen with monitor role First, and the presentation is shown on the screen with monitor role Second.

DualPresentationOnly: All participants in the call are shown on the screen with monitor role First. If a presentation is part of the layout, the presentation is shown on the screen with monitor role Second.

## Video Output Connector [n] CEC Mode

n: 1..2

This video output (HDMI) supports Consumer Electronics Control (CEC).

When this setting is On, the video conferencing device will use CEC to set the screen in standby when the device itself enters standby. Likewise the device will wake up the screen when the device itself wakes up from standby.

The active video input on a screen is sometimes changed by a user. When a call is started the device detects if the active video input has been switched to another input on the screen. The device then switches the input back so the device is the active video input source. If the device is not the active input source when the device goes into standby the screen will not be set to standby.

It's a prerequisite that the screen that is connected to the output is CEC compatible and that CEC is enabled on the screen.

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, INTEGRATOR

Default value: On

Value space: Off/On

Off: CEC is disabled.

On: CEC is enabled.



## Video Output Connector [n] Location HorizontalOffset

n: 1..2

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = "0" and VerticalOffset = "0" indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have two screens side by side. The left screen is on Connector 1 and the right screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "1", VerticalOffset = "0"

Example: You have two screens, one below the other. The upper screen is on Connector 1 and the lower screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "0", VerticalOffset = "-1"

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: "0" Connector 2: "1"

Value space: String (1, 12)

The string represents a decimal number between -100.0 and 100.0 (these numbers included). Input strings that complies with the std::stof function in the C++ <string> library are accepted. This means that you can use either decimal notation or E-notation, for example "12", "12.0", "1.2e1", "1.2E1", "-0.12", "-12e-2". Leading whitespace characters are discarded, and the decimal point is ".".

## Video Output Connector [n] Location VerticalOffset

n: 1..2

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = "0" and VerticalOffset = "0" indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have two screens side by side. The left screen is on Connector 1 and the right screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "1", VerticalOffset = "0"

Example: You have two screens, one below the other. The upper screen is on Connector 1 and the lower screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "0", VerticalOffset = "-1"

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: "0"

Value space: String (1, 12)

The string represents a decimal number between -100.0 and 100.0 (these numbers included). Input strings that complies with the std::stof function in the C++ <string> library are accepted. This means that you can use either decimal notation or E-notation, for example "12", "12.0", "1.2e1", "1.2E1", "-0.12", "-12e-2". Leading whitespace characters are discarded, and the decimal point is ".".

## Video Output Connector [n] MonitorRole

n: 1..2

The monitor role describes which video streams will be shown on the screen connected to this video output. Together the Video Monitors setting and the MonitorRole settings for all outputs define which layout (video streams) will be shown on each screen.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: Auto

Value space: Auto/First/Second/PresentationOnly

Auto: The device will detect when a screen is connected, and a monitor role (First, Second) that corresponds with the Video Monitors setting will be assigned automatically.

First/Second: Define the role of the screen in a multi-screen setup. In a single-screen setup, there is no difference between First and Second.

PresentationOnly: Show presentation video stream if active, and nothing else. Screens/outputs with this monitor role are ignored by the Video Monitors setting.

## Video Output Connector [n] Resolution

n: 1..2

Define the resolution and refresh rate for the connected screen.

The formats larger than 1920\_1200\_60 requires use of high quality display cables. For guaranteed operation, use display cables that are pre-qualified from Cisco for use at 3840\_2160\_60, or use a cable that has passed the "Premium HDMI certification" program.

Some UHD TVs/displays only enable 3840\_2160\_30 (30 Hz) and not 3840\_2160\_60 (60 Hz) as their default configuration. In such cases the corresponding setting on the TV/display must be reconfigured to allow 3840\_2160\_60 for the HDMI input where the device is connected.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Connector n: Auto

Value space: Auto/1920\_1080\_50/1920\_1080\_60/1920\_1200\_50/1920\_1200\_60/2560\_1440\_60/3840\_2160\_30/3840\_2160\_60

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

1920\_1080\_50: The resolution is 1920 x 1080, and the refresh rate is 50 Hz.

1920\_1080\_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

1920\_1200\_50: The resolution is 1920 x 1200, and the refresh rate is 50 Hz.

1920\_1200\_60: The resolution is 1920 x 1200, and the refresh rate is 60 Hz.

2560\_1440\_60: The resolution is 2560 x 1440, and the refresh rate is 60 Hz.

3840\_2160\_30: The resolution is 3840 x 2160, and the refresh rate is 30 Hz.

3840\_2160\_60: The resolution is 3840 x 2160, and the refresh rate is 60 Hz.

## Video Output Connector [n] RGBQuantizationRange

n: 1..2

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. Most HDMI displays expects full quantization range.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Auto, Connector 2: 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, INTEGRATOR

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 third-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: 1/2/3

The video input source to use as default presentation source.

## Video Presentation Priority

Determine how to distribute the bandwidth between the presentation channel and the main video channel.

Requires user role: ADMIN

Default value: Equal

Value space: Equal/High/Low

Equal: The available bandwidth is shared equally between the presentation channel and the main video channel.

High: The presentation channel is assigned a larger portion of the available bandwidth at the expense of the main video channel.

Low: The main video channel is assigned a larger portion of the available bandwidth at the expense of the presentation channel.

## 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, INTEGRATOR

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 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, INTEGRATOR

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 OnMonitorRole

Define which screen/output to display the main video source (self-view) after a call. The value reflects the monitor roles set for the different outputs in the Video Output Connector [n] MonitorRole setting.

The setting applies both when self-view is displayed in full screen, and when it is displayed as picture-in-picture (PiP).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/First/Second

Current: When leaving a call, the self-view picture will be retained on the same output as it was during the call.

First: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to First.

Second: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to Second.

## 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, INTEGRATOR

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, INTEGRATOR

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, INTEGRATOR

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.

## WebEngine settings

### WebEngine Mode

The web engine is a prerequisite for features that use the device's web view, for example digital signage.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The web engine is disabled.

On: The web engine is enabled.

### WebEngine RemoteDebugging

If you encounter a problem with a web page, it can be a good idea to turn on remote debugging. Remote debugging lets you access the Chrome developer console and identify potential issues with a web page. When enabled, a banner is displayed at the bottom of the screen, warning the users that they may be monitored. The banner also shows the URL that you can enter in your local Chrome browser to open the developer console.

Make sure to turn off remote debugging after use.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Remote debugging is switched off.

On: Remote debugging is switched on.

## Experimental settings

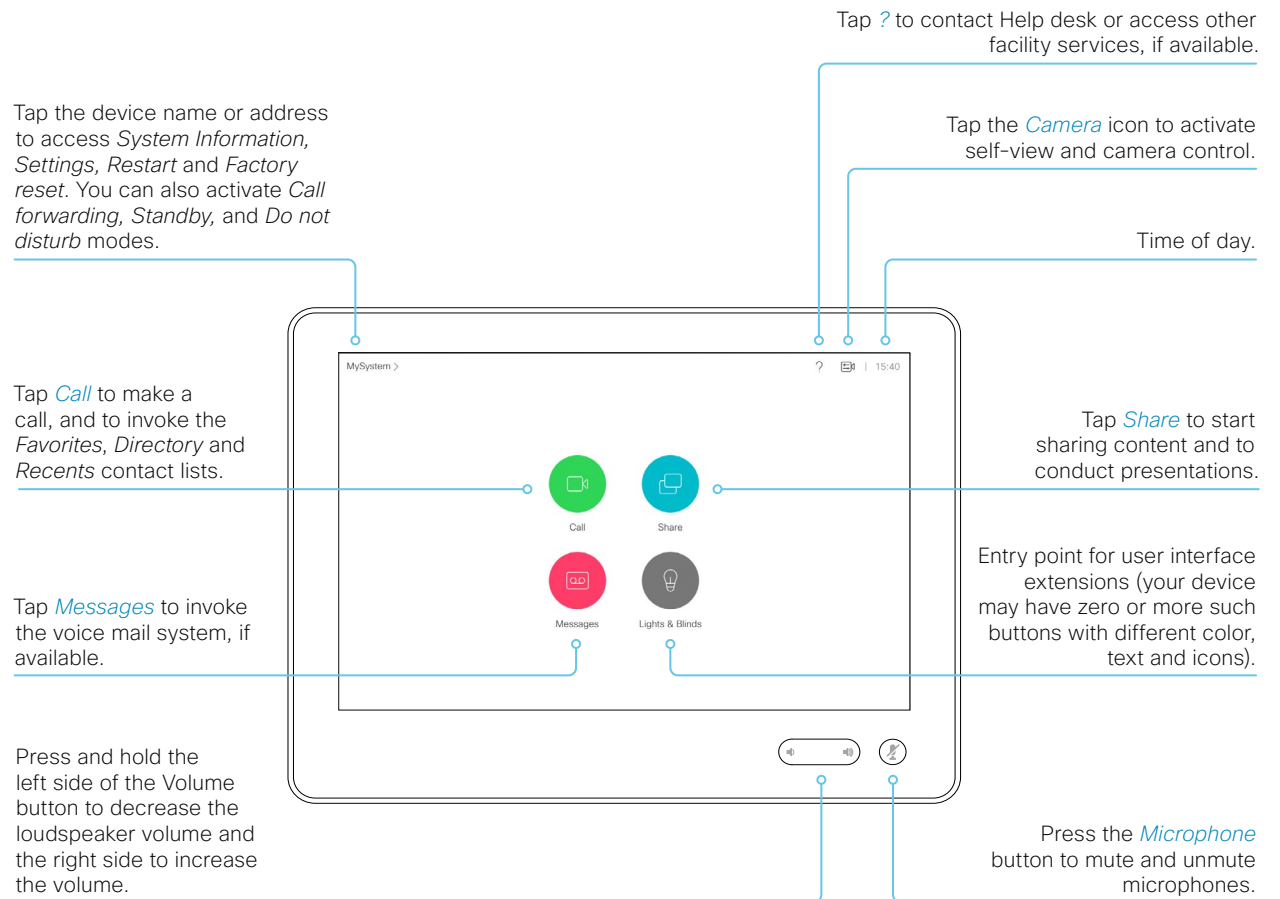
The Experimental settings are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

# Appendices



## How to use Touch 10

The Touch 10 user interface and its use are described in full detail in the User guide for the video conferencing device.



## Set up remote monitoring

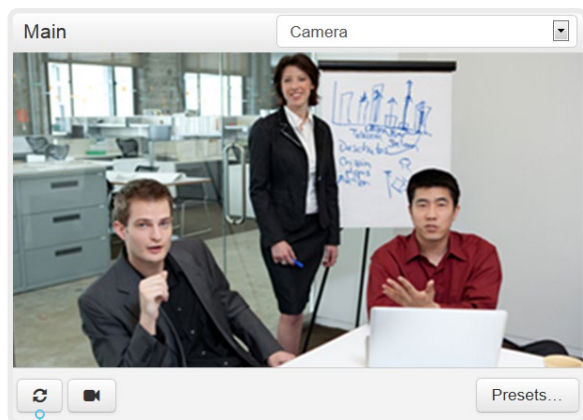
Requirement:

- *RemoteMonitoring* option

Remote monitoring is useful when you want to control the device 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 device 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 DEVICE THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS YOUR RESPONSIBILITY TO COMPLY WITH PRIVACY REGULATIONS WHEN USING THE DEVICE 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 device appear on the Call Control page.

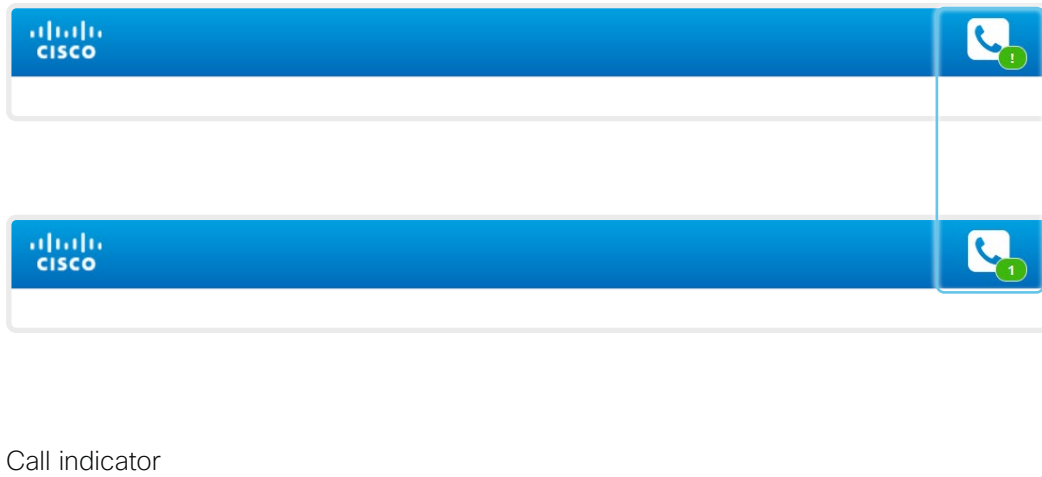
Snapshots appear both when the device is idle, and when in a call.

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 device has the *RemoteMonitoring* option.

Far end snapshots are not displayed if the call is encrypted.

## Access call information and answer a call while using the web interface



### Notification of an incoming call

Click the *Call indicator* to open the *Call Control* page, where you can accept or decline the call.

### The device is in a call

The badge indicates the number of active calls.





### Call indicator

The call indicator is present to notify you about an incoming call, and to show when the device is in a call.

If the device is idle, there is no call indicator.

### Control the call

Relevant control buttons are present on the *Call Control* page. Use the buttons to:

-  Show call details
-  Put the call on hold
-  Answer the call
-  Disconnect the call

## Place a call using the web interface (page 1 of 2)

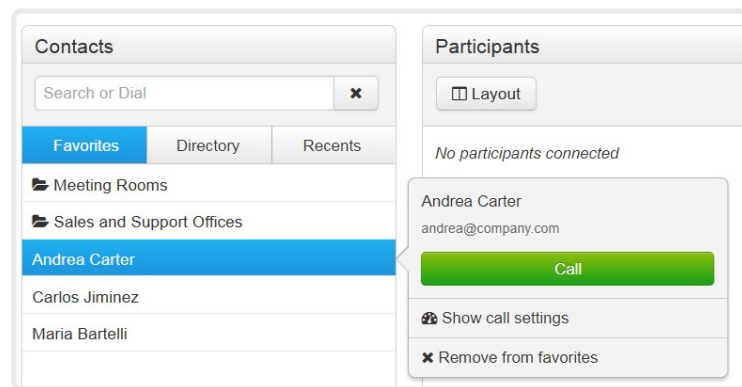
Sign in to the web interface and navigate to [Call Control](#).

### Place a call

**i** Even if the web interface is used to initiate the call, it is the video conferencing device (display, microphones and loudspeakers) that is used for the call; it is not the PC running the web interface.

1. Navigate the *Favorites*, *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.

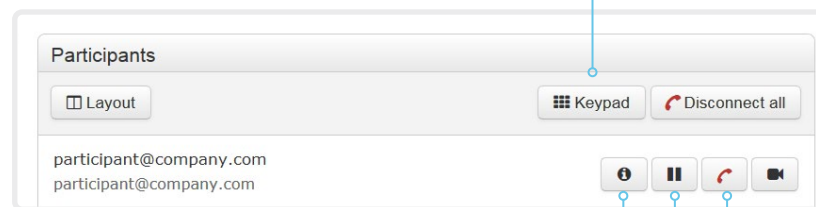
Alternatively, enter the complete URI or number in the *Search and Dial* field. Then click the [Call](#) button that appears next to the URI or number.



\* When searching, matching entries from the *Favorites*, *Directory* and *Recents* lists will be listed as you type.

### 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 or conference, click [Disconnect all](#). Confirm your choice in the dialog that appears.

To disconnect just one participant in a conference, click the button for that participant.

## Place a call using the web interface (page 2 of 2)

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

### Calling more than one

A point-to-point video call (a call involving two parties only) can be expanded to include one more participant on audio-only.

If your device is using the optional built-in MultiSite feature, up to four participants, yourself included, can join the video call (conference).

Follow the same procedure to call the next conference participant as you did when calling the first participant.

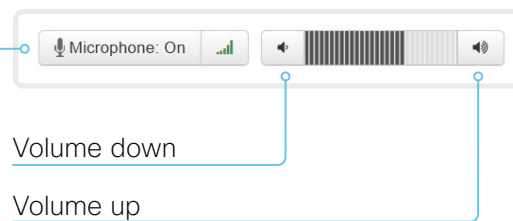
Calling more than one using a conference bridge is not supported from the web interface, even if it is supported by the video conferencing device itself.

### 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

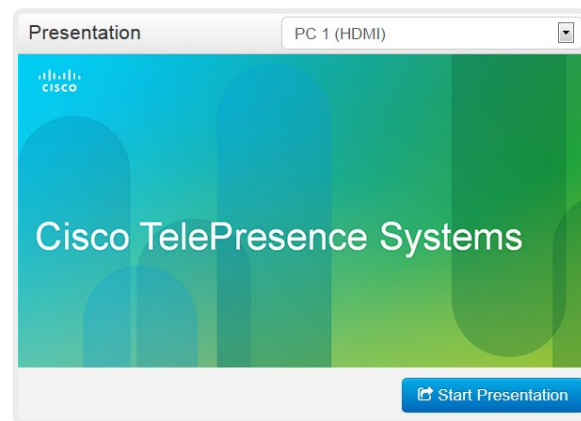
Sign in to the web interface and navigate to [Call Control](#).

### 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 devices that have the *Remote Monitoring* option.

### About content sharing

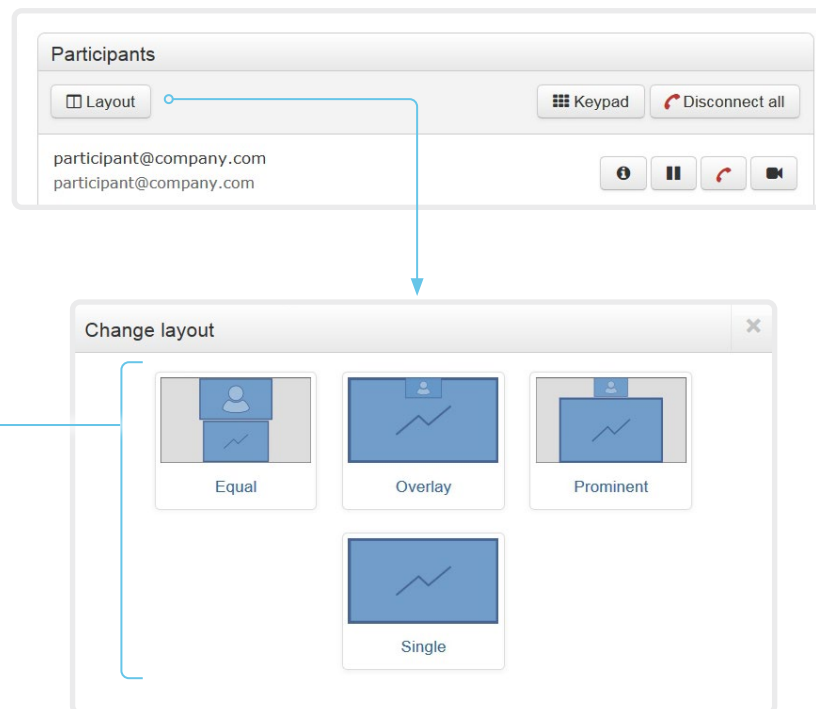
You can connect a presentation source to one of the video inputs of your device. Most often a PC is used as presentation source, but other options may be available depending on your device setup.

While in a call you can share content with the other participant(s) in the call (far end).

If you are not in a call, the content is shown 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 device configuration.

You may change the layout both when idle and in a call.

### About layouts

The term layout is used to describe the various ways presentations and videos can appear on the screen. Different types of meetings may require different layouts.

The number of call or conference participants are reflected in the available choices.

\* Changing the participant layout from the web interface is not supported when calling a conference bridge, even if it is supported on the video conferencing device itself.

## 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.
- Speaker tracking is switched Off.

### Snapshot area

Shows snapshots of the selected main input source.

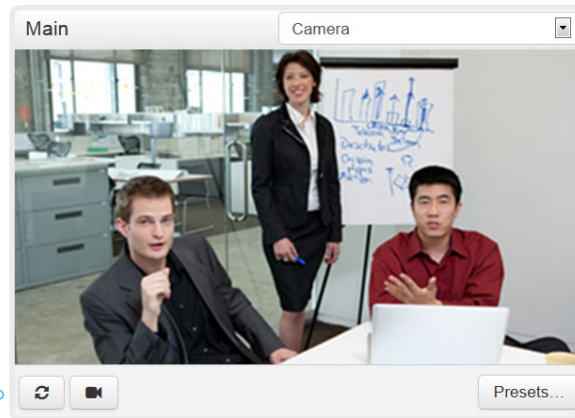
Only available on devices that have the *Remote Monitoring* option.

### Automatically refresh snapshots

### Move the camera using the pan/tilt/zoom controls

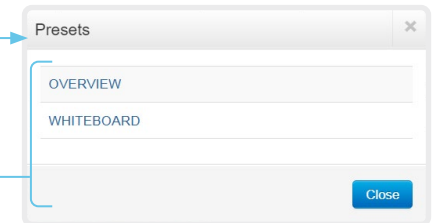
Camera control is not available when speaker tracking is switched on.

1. Choose which camera to control in the *Main* source drop down list.
2. Click the camera icon to open the camera control window.  
Video snapshots from the room are only displayed for devices that have the *Remote Monitoring* option.
3. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.  
Only relevant controls appear in the window.
4. Click [Close](#) to close the window.



### Main source drop down list

Choose which camera to control from the drop down list.

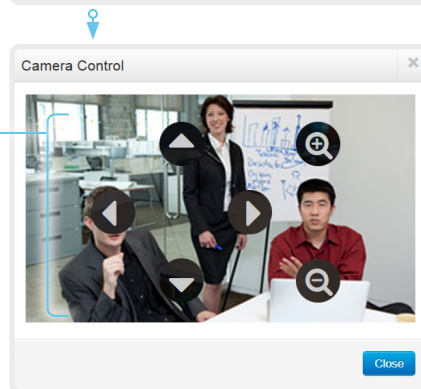


### Move the camera to a preset position

1. Choose which camera to control in the *Main* source drop down list.
2. Click [Presets...](#) to open a list of available presets.  
If no presets are defined, the button is disabled and named *No presets*.
3. Click a preset's name to move the camera to the preset position.
4. Click [Close](#) to close the window.

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

When you select a preset, speaker tracking will be switched off automatically.





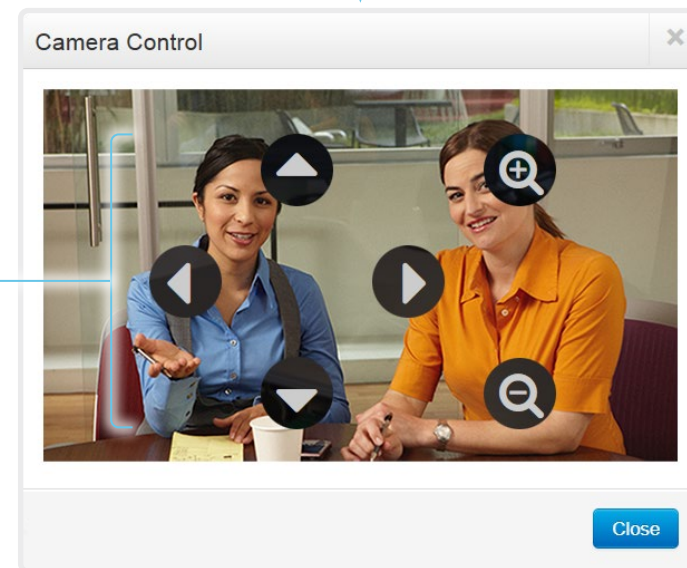
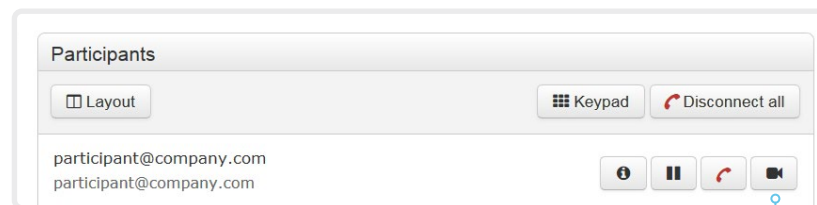
## Control a far end camera

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 device.
- The far end camera has pan, tilt or zoom functionality. Only the relevant controls will appear.
- Speaker tracking is not switched On on the far end camera.
- The local device 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.

## Packet loss resilience - ClearPath

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

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

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

## Room analytics (page 1 of 2)

The room analytics feature use several variables from the conference room and re-uses them to analyze the room utilization over time or per call.

### People presence detection

The device has the capability to find whether or not people are present in the room. It takes a minimum of two minutes to detect whether people are present or not in the room. After the room becomes vacant, it may take up to two minutes for the status to change.

This feature is based on ultrasound. It will not keep record of who was in the room, only whether or not there are people present in the room.

You can turn the people presence detection on or off from the web interface. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > PeoplePresenceDetector](#).

### People count

Applies when using a Quad Camera.

By using face detection, the device can find how many persons are in the room. It will not keep record of who was in the room, only the average number of faces that were detected. Persons that have not faced the camera will not be counted. If there are objects or pictures in the room that can be detected as faces these might be counted.

The call must have a duration of minimum two minutes in order to get a reliable average. Calls that last less than two minutes, and calls which are made with people count disabled, will display "N/A" when you retrieve call history.

By default, the device only counts people when in a call, or when it displays the self-view picture.

You can choose to count people outside of call. When enabled, the device counts people as long as the device is not in standby mode. This includes outside of call, even if self-view is off. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > PeopleCountOutOfCall](#).

### Status

You may see the status at a given moment of people's presence and people count. Sign in to the web interface and navigate to [Setup > Status > RoomAnalytics](#).

### Diagnostics

You can see the live people counter on-screen by enabling the SpeakerTrack Diagnostics mode from the Touch 10 controller. Turn on selfview, and tap the device name or address at the top of the user interface and open the [Settings](#) menu. Tap [Issues & diagnostics](#) and switch on [SpeakerTrack diagnostics](#).

### Call history command

After a call the average people count value can be extracted from the Call History command.

- `xCommand CallHistory Get DetailLevel: Full`

The Call History command is available from the API (Application Programming Interface). Refer to the API Reference Guide for your product to for details.

Go to: ► <https://www.cisco.com/go/room-docs>

## Room analytics (page 2 of 2)

### Ambient noise reporting

The devices can report the stationary ambient noise level in the room. The reported value is an A-weighted decibel value (dBA), which reflects the response of the human ear. All signal processing related to this feature is local, the only data transmitted is the calculated noise level.

This value can be used to detect abnormal changes to the noise level. Such changes may be caused by noise that can be an annoyance for people working in the room. Facility management can then quickly intervene to troubleshoot the issue.

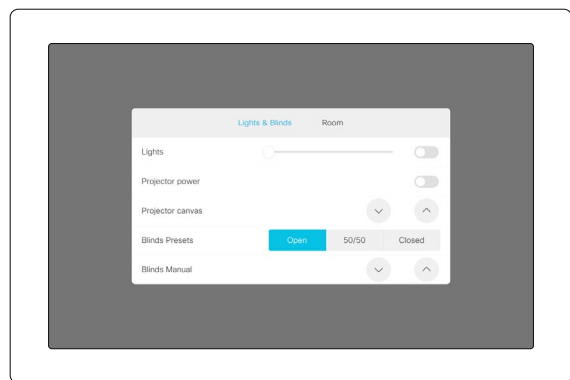
You can turn the ambient noise detection on or off from the web interface. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > AmbientNoiseEstimation > Mode](#).

Customization

# Customize the video conferencing device's Touch 10 user interface (page 1 of 2)

You can customize the user interface to allow control of peripherals in a meeting room, for example lights and blinds, or to modify the video conferencing device's behavior by triggering macros.

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



Example in-room control panel

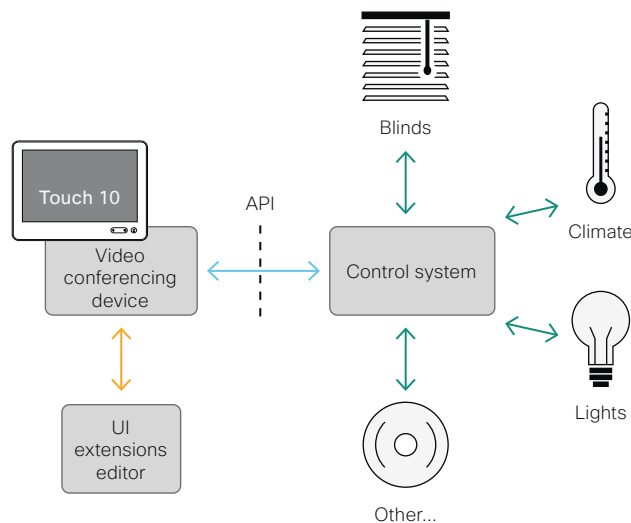
Consult the *Customization guide* for full details about how to design custom user interface panels and action buttons using the UI Extensions editor (formerly In-Room Control editor), and how to use the video conferencing device's API to program the controls and actions. Go to:

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

## In-room control architecture

You need a Cisco video conferencing device with a Touch 10 controller, and a control system. The control system may be a third-party system, such as Crestron or AMX, with hardware drivers for peripherals. It is the control system, not the video conferencing device, that controls the peripherals.

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



In-room control schematics

The video conferencing device's macro framework may also serve as a control system. In this case the control system can use the device's API to trigger all sorts of local functionality: Speed dial, language selection, customized system reset, and much more.

Customization


## Customize the video conferencing device's Touch 10 user interface (page 2 of 2)

### The UI Extensions editor

#### Free of charge editor

An easy to use drag-and-drop editor, which you should use to compose the custom user interface extensions (action buttons and custom panels such as in-room controls), comes free of charge with the video conferencing device's software.

Sign in\* to the web interface and navigate to [Integration > UI Extensions Editor](#).

- The editor opens directly in the device's web interface.  
You can create and push a new panel or action button to the device, and see the result immediately on its user interface.
- Click the Editor menu  and select [Download the Editor](#) to get a stand-alone version that you can run locally in your browser from your hard drive.

Then you can compose your custom interfaces without being connected to a device. You can export and import to file to move your work between your local version and the device later.

#### Preview function

The editor also provides a preview function, which allows you to see how the custom interfaces will appear on the user interface.

The preview function is also a complete software version of your custom panels, so clicking the controls will result in the same actions as selecting them on the real Touch 10 user interface.

Therefore, you can use the preview function to test your integrations without having a real Touch 10 user interface available. You can also use the device's custom panels from a remote location.

---

\* You need a user that holds the ROOMCONTROL, INTEGRATOR, or ADMIN user roles in order to access the UI Extensions editor and the API commands that you need when programming.

Customization

## Customize the video conferencing device's behavior using macros

With macros, you can create your own snippets of code that run on the device. The language is JavaScript / ECMAScript 6 with support for features such as arrow functions, promises and classes.

The macro framework allows an integrator to write scripts that tailor a device's behavior to suite an individual customer's requirements. The integrators can, for example, implement their own features or variations of features, automate specific configurations or re-configurations, and create custom tests and monitoring functions.

By combining the use of macros and creation of a custom user interface panel (UI extension), you can amend the user interface (Touch 10) to trigger customized local functionality. For examples:

- Add speed dial buttons
- Add a button for room reset, which set all configurations back to your preferred default setup

Consult the *Customization guide* for details about macros and how to use the device's built in Macro editor. Go to:

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

### Allow using macros on the device

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

- Set [Macros > Mode](#) to **On**.

If you try to launch the Macro editor while this setting is **Off**, a pop-up message appears. If you respond by tapping [Enable Macros](#), the [Macros > Mode](#) setting will automatically change to **On**, and the editor will launch.

### Launch the macro editor

Sign in\* to the web interface and navigate to [Integration > Macro Editor](#).

We don't offer a stand-alone version of the editor that you can use to work offline.

### The Macro editor

The Macro editor is a powerful tool where you can:

- Load our code examples, which you can modify, use as is, or use as inspiration when writing your own macros.
- Read our detailed macro scripting tutorial, which also explains the code examples in more detailed.
- Write your own macros, and upload them to the device.
- Enable/Disable individual macros.
- Check in an embedded Log Console what happens when you run a macro.

\* You need a user that holds the ADMIN user role in order to access the Macro editor.

Customization

## Remove default buttons from the user interface

In some use cases, you may never use a default button, like *Call* or *Share*. Such unused buttons may cause confusion. In these cases, you can remove the unused buttons from the user interface. Custom UI buttons can be exposed still. Removing default buttons while adding custom buttons makes it possible fully to customize the user interface.

For example, you can remove the *Call* and *Share* buttons if nobody is going to share content or call from this device. Instead, add custom buttons and panels for the tasks that are going to be performed.

### Configurations

Use the following configurations to remove default buttons from the user interface . The configurations are available both from the web interface of the device, and in the API.

- *UserInterface > Features > Call > Start*: Removes the default *Call* button (including the directory, favorites, and recent calls lists). Also removes the *Add* participant button while in a call.
- *UserInterface > Features > Share > Start*: Removes the default user interface for sharing and previewing content, both in call and out of call.
- *UserInterface > Features > Call > VideoMute*: Removes the default *Turn video off* button.
- *UserInterface > Features > HideAll*: Removes all the default buttons. Custom buttons are not removed.
- *UserInterface > Features > Call > End*: Removes the *End Call* button.
- *UserInterface > Features > Call > MidCallControls*: Removes the *Hold*, *Resume*, and *Transfer* in-call buttons.



The configurations remove only the buttons, not the functionality as such. You can share content using Proximity, even if you have removed the *Share* button from the user interface.

### Further Information

Find more details about how to remove buttons and customize the user interface in the *Customization guide*. Go to:

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



Customization

## Use of a third-party USB input device

You can use a third-party USB input device to control certain functions on video conferencing device. A Bluetooth remote control (with a USB dongle) and a USB keyboard are examples of such input devices.

This feature is meant to complement the functionality of the Touch 10 or the DX user interfaces, wherever convenient. It is not meant to replace the Touch 10 and DX user interfaces.

Examples of applications:

- In classrooms and during lectures, a small remote control can be used to wake up a video conferencing device from standby mode. Also, it may be convenient to use a remote control to select which input source to present.
- Controlling the camera view (pan, tilt, and zoom) in situations where you are not allowed to use the Touch 10. For example, in operating rooms in a hospital.

### Functional Overview

Pressing a button on the USB input device, generates an event in the API. Macros or third-party control devices can listen for such events, and respond to them. This behavior is similar to the behavior of custom UI buttons (UI extensions). It is also possible to listen for the events using webhooks, directly in an SSH session.

There isn't a library of actions readily available to select actions from. You must define and implement the actions to be taken as response to the events yourself. For example:

- Increase the volume of the video conferencing device when the Volume Up key is pressed.
- Put the video conferencing device in standby mode when the Sleep key is pressed.

### Configurations, Events, and Status

The support for third-party USB input devices is disabled by default. Enable it explicitly by setting the *Peripherals > InputDevice > Mode* to **On**.

Pressing and releasing a button generates a Pressed and a Released event:

```
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Pressed
** end
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Released
** end
```

To listen for events, you must register feedback from the InputDevice events:

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

When the video conferencing device detects the third-party input device, the input device is listed in the video conferencing device's *UserInterface > Peripherals > ConnectedDevice* status. The input device may be reported as multiple devices.

### Required Equipment

- A device from the Cisco Webex Room Series or DX Series.
- A third-party input device that advertises itself as a USB keyboard, for example a Bluetooth remote control with a USB dongle.

### Further Information

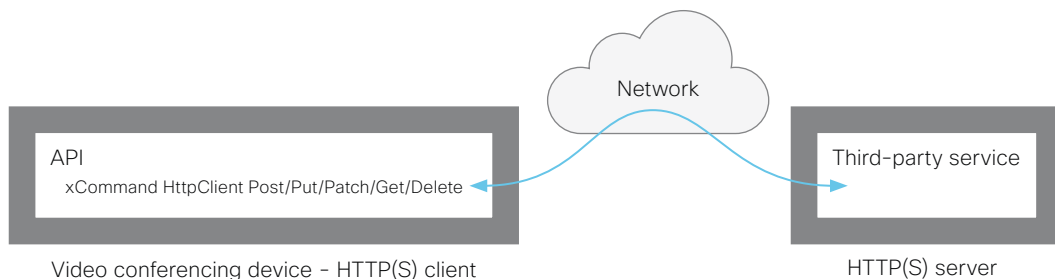
Find more information about the use of a third-party input device in the *Customization guide*. Go to:

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

Cisco support (TAC) doesn't support debugging of third-party code, including macros. Please check the ► [Cisco Collaboration Developer community](#) if you need help with macros and third-party code.

Customization

## Sending HTTP(S) requests



The HTTP(S) request feature makes it possible to send arbitrary HTTP(S) requests from a video conferencing device to an HTTP(S) server. Furthermore, the device receives the response that the server sends back. The device supports the **Post, Put, Patch, Get, and Delete** methods.

By using macros, you can send data to an HTTP(S) server whenever you want. You can choose what data to send, and structure them as you like. By doing it this way, you can adapt the data to an already established service.

Security measures:

- The HTTP(S) request feature is disabled by default. A system administrator must explicitly enable the feature by setting `HttpClient > Mode` to **On**.
- The system administrator can prevent the use of HTTP by setting `HttpClient > AllowHTTP` to **False**.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent HTTP(S) requests is limited.

### List of Allowed HTTP(S) servers

The system administrator can use these commands to set up and maintain a list of up to ten allowed HTTP(S) servers (hosts):

- `xCommand HttpClient Allow Hostname Add Expression: <Regular expression that matches the host name or IP address of the HTTP(S) server>`
- `xCommand HttpClient Allow Hostname Clear`
- `xCommand HttpClient Allow Hostname List`
- `xCommand HttpClient Allow Hostname Remove Id: <id of an entry in the list>`

If the list is not empty, you can send HTTP(S) requests only to the servers in the list. If the list is empty, you can send the requests to any HTTP(S) server.

The check against the list of allowed servers is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

### HTTPS without certificate validation

When sending requests over HTTPS, the video conferencing device checks the certificate of the HTTPS server by default. If the HTTPS server certificate is not found to be valid, you get an error message. The device doesn't send any data to that server.

We recommend using HTTPS with certificate validation. If certificate validation is not possible, the system administrator can set `HttpClient > AllowInsecureHTTPS` to **On**. This allows the use of HTTPS without validating the certificate of the server.

### Sending HTTP(S) requests

Once the HTTP(S) request feature is enabled, you can use the following commands to send requests to an HTTP(S) server:

```
xCommand HttpClient <Method>
  [AllowInsecureHTTPS: <True/False>]
  [Header: <Header text>]
  [ResponseSizeLimit: <Maximum response size>]
  [ResponseBody: <None/PlainText/Base64>]
  [Timeout: <Timeout period>]
  Url: <URL to send the request to>
```

where <Method> is either Post, Put, Patch, Get, or Delete.

The Post, Put, and Patch commands are multiline commands. Read the API guide to find out how to use multiline commands, and also to find a detailed description of the command parameters

### Further information

Find more information about HTTP(S) Post requests in the *Customization guide*. Go to:

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

Web view based features

## Digital signage

Digital signage allows you to show custom content (a web page) on a device when it's in half-wake state. Digital signage is a way to display advertising content and promote your brand, but also to show visitor and internal employee information, dashboards, or calendars.

The content replaces the traditional half-wake background image and information, and is always shown on full screen. Only one web window or tab is supported. If a web page tries to open a page in a new window or tab, it replaces the current page.

Data, such as cache, cookies, and local storage, is NOT automatically cleared when the device restarts. You must use the delete storage command to delete the data.

- `xCommand WebEngine DeleteStorage [Type: WebApps]`

If a web page is not supported, the device goes directly to normal half-wake mode. You can see more information in the [Maintenance > Diagnostics](#) page in the web interface of the device.

## Set up digital signage

1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Set [WebEngine > Mode](#) to **On** to enable the web engine.
3. Set [Standby > Signage > Mode](#) to **On** to enable digital signage.
4. Enter the URL of the web page that you want to show in [Standby > Signage > Url](#).
5. The web page is shown *before* the device enters standby mode. Use the following settings to determine for how long the web page is shown.

[Standby > Mode](#): If set to **Off**, the device never enters standby mode (not recommended). If set to **On**, the device enters standby mode when the [Standby > Delay](#) has timed out.

[Standby > Delay](#): Define how long (in minutes) the device shows the web page before going into standby mode.

[Standby > WakeUpOnMotionDetection](#): If set to **On**, the device wakes up automatically from standby, and starts showing the web page when people enter the room. If set to **Off**, the device is not affected by people entering the room.

Other digital signage settings:

- Decide whether to play out the audio for web pages that have audio.  
[Standby > Signage > Audio](#)
- Force a web page to refresh at regular intervals. This is useful for web pages that don't refresh themselves.  
[Standby > Signage > RefreshInterval](#)

## The web engine

All web view based features are using the web engine. Therefore the web engine must be enabled before you can use a web view based feature.

The web engine is based on Chromium / Qt WebEngine with V8 JavaScript. The Chromium version is updated regularly, but it might be older than your Chrome laptop version.

These features are not supported: PDF, WebGL WebRTC, password manager, plug-ins, downloading and uploading files, and notifications.

## Remote debugging

If you encounter a problem with a web page, you can turn on remote debugging.

[WebEngine > RemoteDebugging](#)

Remote debugging lets you access the Chrome developer console and identify potential issues with a web page. When enabled, a banner is displayed at the bottom of the screen, warning the users that they may be monitored. The banner also shows the URL that you can enter in your local Chrome browser to open the developer console.

Web view based features

## API-driven web views

Web views can be opened and closed using API commands. Integrators can use these commands when making third-party integrations or macros. The integrator decides which URL to load based on external events. An example is to show important company alerts.

The web view is fullscreen and will time out after 15 minutes, or by calling the API command to close the view.

Open the web view:

- `xCommand UserInterface WebView Display Url: <url>`

Close the web view:

- `xCommand UserInterface WebView Clear`

Data, such as cache, cookies, and local storage, is automatically cleared when the session ends.

By combining API-driven web views, macros, and custom buttons on the Touch controller, an integrator can make interactive solutions also for devices without touch screens. Tapping different buttons on the Touch controller shows different web views on the main screen. For example to open and browse basic help pages or show instructional videos.

## The web engine

All web view based features are using the web engine. Therefore the web engine must be enabled before you can use a web view based feature.

The web engine is based on Chromium / Qt WebEngine with V8 JavaScript. The Chromium version is updated regularly, but it might be older than your Chrome laptop version.

These features are not supported: PDF, WebGL WebRTC, password manager, plug-ins, downloading and uploading files, and notifications.

## Remote debugging

If you encounter a problem with a web page, you can turn on remote debugging.

[WebEngine > RemoteDebugging](#)

Remote debugging lets you access the Chrome developer console and identify potential issues with a web page. When enabled, a banner is displayed at the bottom of the screen, warning the users that they may be monitored. The banner also shows the URL that you can enter in your local Chrome browser to open the developer console.

## Input source composition (page 1 of 2)

You can use the device's API to combine up to four input sources in a single main video stream.

The maximum number of *different* input sources depends on the device:

Video conferencing device	Maximum number of different input sources
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2	2
Codec Plus, Room 55, Room 55 Dual, Room 70	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	4
SX10, DX70, DX80	Not applicable

## Source composition

### Composition layout

You can choose between three layouts:

- Equal
- Prominent
- PIP (only available when composing two input sources)

You can modify the PIP position to one of the corners. The size of the PIP can be normal or large.

The composition and layout can be modified at any time, both in call and outside of call.

### Selfview

Selfview shows the same composed image that is being sent to the far end.

### Individual camera control

You can control individual cameras using API commands (`xCommand Camera *`), but you cannot use the controls on the user interface.

When you select a camera in the user interface, the main video stream will automatically switch from the composed video stream to the single stream from the chosen camera.

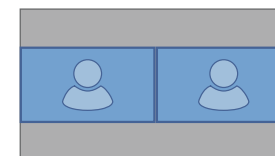
### Change compositions and layouts on demand

Input source composition is only available using API commands; we don't provide a dedicated user interface for it.

To be able to easily change compositions and layouts on demand, we recommend that you use macros and create a custom user interface panel (UI extension) for it.

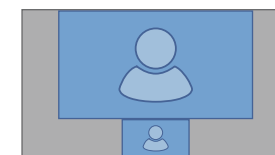
## Layouts

### Equal



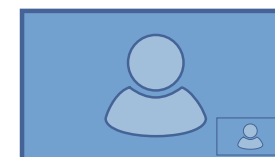
Number of sources: 2

### Prominent

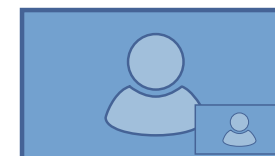


Number of sources: 2

### Picture-in-Picture (PIP)



Lower right corner



Lower right corner, large PIP

## Input source composition (page 2 of 2)

### API command

```
xCommand Video Input SetMainVideoSource
ConnectorId: <1..n> SourceId: <1..m>
Layout: <Equal, PIP, Prominent>
PIPPosition <LowerLeft, LowerRight,
UpperLeft, UpperRight>
PIPSize <Auto, Large>
```

where

The input source can be identified by either the physical connector that it is connected to (ConnectorId), or by the logical source identifier (SourceId). There cannot be a mix of different types of identifiers in the same command; use either ConnectorId or SourceId. You can find these identifiers in the *Video Input Connector* and *Video Input Source* statuses.

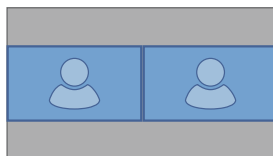
The difference between the equal, PIP, and prominent layouts (Layout) are shown in the sidebar.

You can modify the PIP position to one of the corners. The size of the PIP can be normal (auto) or large.

Refer to the API-guide for more details.

### Examples

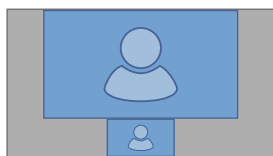
```
xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 Layout: Equal
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP PIPPosition: LowerRight PIPSize: Large
```



```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: Prominent
```



## Presentation source composition (page 1 of 2)

You can use the device's API to combine up to four presentation sources in a single video stream.

The maximum number of *different* presentation sources depends on the device:

Video conferencing device	Maximum number of different presentation sources
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2, Board	2
Codec Plus, Room 55, Room 55 Dual, Room 70	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	4
SX10, DX70, DX80	Not applicable

You can only share sources that has been shared through a cable (DVI, VGA, HDMI - depending on the device).

### Source composition

#### Composition layout

You can choose between two layouts:

- Equal
- Prominent

You can change the number of sources at any time, both in call and outside of call. The image sizes cannot be modified.

The order in which the sources appear on the screen depends on the order they have in the command; starting from upper left, ending at bottom right.

#### Change compositions and layouts on demand

Presentation source composition is only available using API commands; we don't provide a dedicated user interface for it.

To be able to easily change compositions and layouts on demand, we recommend that you use macros and create a custom user interface panel (UI extension) for it.

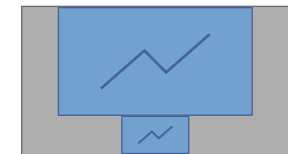
### Layouts

#### Equal



Number of sources: 2

#### Prominent



Number of sources: 2

## Presentation source composition (page 2 of 2)

### API command

```
xCommand Presentation Start
  ConnectorId: <1..n>
  PresentationSource: <1..n>
  Instance: <New, 1..n>
  Layout: <Equal, Prominent>
  SendingMode: <LocalRemote, LocalOnly>
```

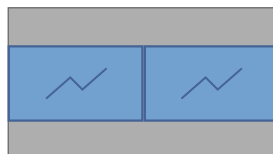
where

The input source can be identified by either the physical connector that it is connected to (ConnectorId), or by the logical source identifier (PresentationSource). There cannot be a mix of different types of identifiers in the same command; use either ConnectorId or PresentationSource. You can find these identifiers in the *Video Input Connector* and *Video Input Source* statuses.

Refer to the API-guide for more details.

### Examples

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```



```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```



```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 ConnectorId: 3 Layout: Equal
```



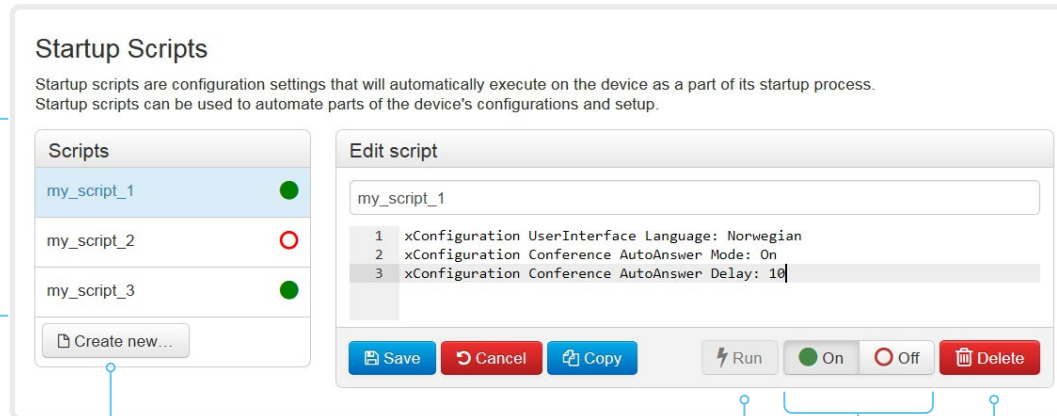
```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 PresentationSource: 3 Layout: Prominent
```





## Manage startup scripts

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



The script names and configurations shown in the illustration serve as examples. You may make your own 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](#).

### 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 device 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 device's XML files

Sign in to the web interface and navigate to [Integration > Developer API](#).

The XML files are part of the device's API. They structure information about the device in a hierarchy.

- *Configuration.xml* contains the current device 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 device 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 device to perform an action. The commands are issued from the API.
- *Valuespace.xml* contains an overview of all the value spaces of device 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 device. The API is described in detail in the API guide for the device.

## 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 device.

### 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

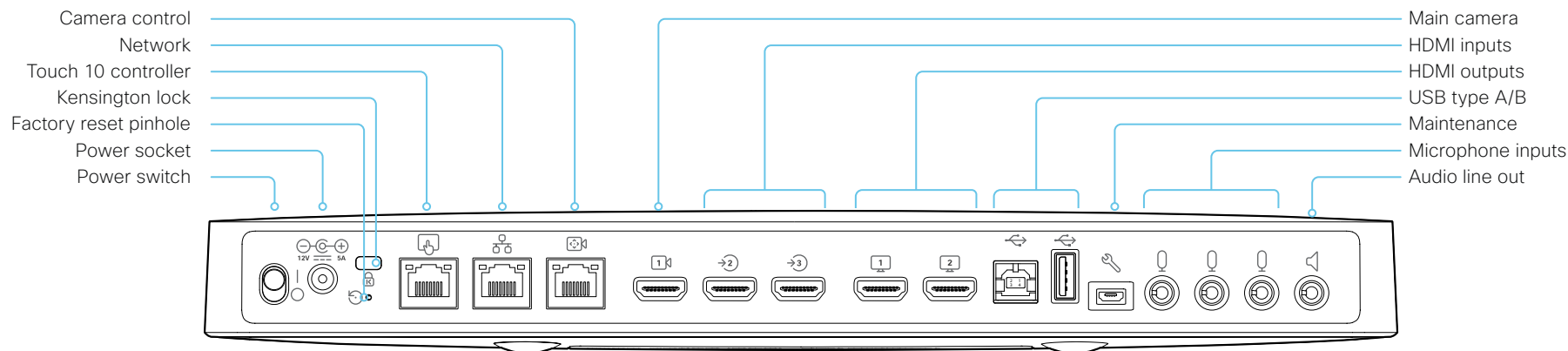
Enter commands...

Execute

### About the API

The application programming interface (API) is a tool for integration professionals and developers working with the device. The API is described in detail in the API guide for the device.

## Connector panel



### Power

Always use the provided power supply:

- DC output: 5A, 12 V
- AC input: 100-240V, 50-60Hz, max 1.2A

The device powers up automatically, as long as the power switch is in its On position.

### Factory reset pinhole

Use the pinhole as a last resort. We recommend to perform a factory reset from the Touch user interface or the web interface.

### Kensington lock

The Kensington lock may be used to prevent the device from being moved and to prevent theft.

### Touch 10 controller

Touch 10 is powered over Ethernet (PoE), which is provided through this socket.

### Network

Ethernet interface, 10Mb/100Mb/1Gb Ethernet LAN interface (RJ45).

### Camera control

Camera control (pan, tilt, zoom) for the camera. If you connect an extra camera you need an Ethernet switch to allow for camera control on both cameras.

### HDMI inputs

HDMI version 1.4b, resolutions up to 3840 × 2160 at 30fps. Used for different types of input sources, like computers, extra camera or external playback devices (audio and video). You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable. The second HDMI input connector allows display of HDCP (High-bandwidth Digital Content Protection) encrypted content.

### HDMI outputs

HDMI version 2.0, resolutions up to 3840 × 2160 at 60fps. Use output 1 for the main monitor and output 2 for the optional second monitor. You need Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables.

There is no audio on the HDMI outputs if the connected

camera has loudspeakers (Quad Camera). Otherwise there is audio on Connector 1.

### HDMI input for the main camera

Always use the HDMI 1 for the main camera.

### USB

USB 2.0 type A/B.

### Maintenance

Micro USB connector for serial communication with the device.

### Microphones

Three 3.5 mm mini-jack, 4-pin connectors for external microphones: Cisco Table Microphone 20 or Cisco TelePresence Ceiling Microphone.

### Audio line out

3.5 mm mini-jack, 3-pin connector. To be used with active loudspeakers (built-in amplifier).

## About Ethernet ports

### The main network port

The main network port – Network port 1 – is always reserved for the connection to LAN. This applies to all video conferencing devices.

Depending on the device, Network port 1 is marked with the number 1, the network symbol (🌐), or both.

### Auxiliary network ports

Some video conferencing devices have more than one network port. The additional ports can be used for peripheral devices like cameras, Touch 10, third-party control systems, and more.

A device that is connected to such a network port gets a local IP address from the codec, and therefore is not part of the corporate network. It is not possible for packets to traverse the codec between the main network port (LAN) and the auxiliary network ports (link-local).

- A Cisco peripheral device is assigned a dynamic IP address in the range (DHCP): 169.254.1.41 to 169.254.1.240
- A non-Cisco device is assigned the dynamic IP address (DHCP): 169.254.1.30

**NOTE:** Only one non-Cisco device can get a dynamic IP address at a time.

- A non-Cisco device can be assigned a static IP address in the range: 169.254.1.241 to 169.254.1.254

This method can also be used to connect to the codec with SSH. In this case you can use the IP address 169.254.1.1.

### Power over Ethernet (PoE)

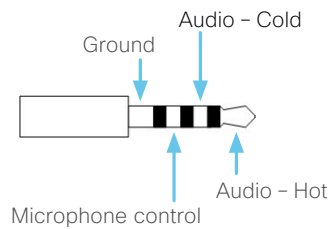
Some of the auxiliary network ports provide Power over Ethernet (PoE). These ports can power peripherals like the Touch 10 controller.

Product	Number of auxiliary network ports	Number of auxiliary network ports with PoE
Room Kit	1	0
Room Kit Mini	1	1 (🌐)
Room 55	1	1 (🌐)
Room 70 / Room 55 Dual	2	1 (🌐)
Room 70 G2	4	2 (🌐, PoE)
Codec Plus	2	1 (🌐)
Codec Pro	4	2 (🌐, PoE)
Boards	0	0
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700 / MX800	2	0*
DX70 / DX80	1	0

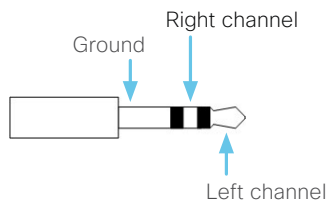
\* These products have a separate PoE injector that is connected to one of the auxiliary network ports. The PoE injector is used for the Touch 10 controller.

## Mini-jack connector pin-out schemes

3.5 mm mini-jack, 4-pin (microphone)



3.5 mm mini-jack, 3-pin (line-out)



Audio connectors (mini-jack)		
	Microphone	Line-out
Connector pin out	Tip = Hot Ring 1 = Cold Ring 2 = Mic. control Shield = GND	Tip = Left channel Ring = Right channel Shield = GND
Signal type	Balanced	Unbalanced
Connector (codec)	Mini-jack 3.5 mm, 4-conductor	Mini-jack 3.5 mm, 3-conductor
Input impedance	900 Ohm/leg	N/A
Output impedance	N/A	470 Ohm
Maximum input level	-18.3 dBu ±2 dB	N/A
Maximum output level	N/A	8.2 dBu ±2 dB
Phantom power	10V ± 0.5V	N/A
Phantom power resistor pin "tip"	1.0 kOhm	N/A
Phantom power resistor pin "ring 1"	1.0 kOhm	N/A
Frequency response	20 Hz-20 kHz ±1 dB	20 Hz-20 kHz ±1 dB
Signal to Noise Ratio	-95 dB	-100 dB

## Serial interface for maintenance

Use the micro USB connector for direct communication with the device<sup>1</sup>. 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<sup>2</sup>.

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
- Hardware flow control: Off

### Device settings

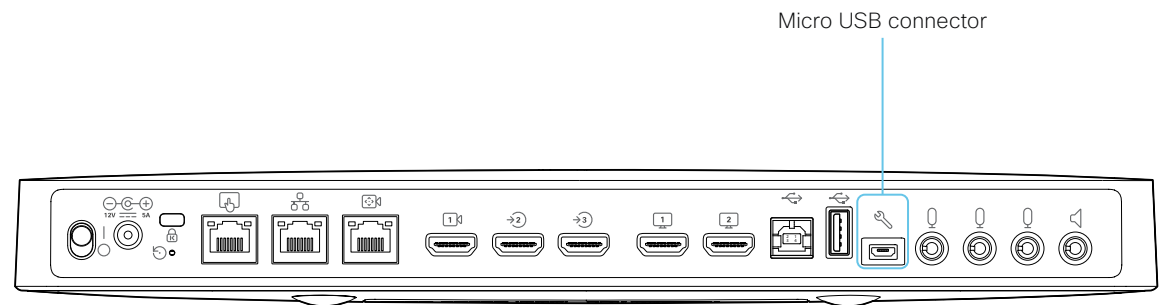
Serial communication is enabled by default. Use the following configuration to change the behavior:

*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*

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



<sup>1</sup> The micro-USB port is for maintenance. If you want to access the device's API over a serial connection, connect to the USB port (type A). Refer to the API guide for details.

<sup>2</sup> You need a CP210x USB to UART Bridge Virtual COM Port (VCP) driver, see <http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

## Open TCP Ports

The web server within the codec prohibit or restrict the use of nonsecure or unnecessary ports, protocols, modules, and/or services. Some ports are open by default.

### TCP 22: SSH

You can close the port by setting SSH mode to **Off**.

```
NetworkServices SSH Mode: Off/On
```

### TCP 80: HTTP

You can close the port by setting HTTP mode to **Off** or **HTTPS**.

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

### TCP 443: HTTPS

You can close the port by setting HTTP mode to **Off**.

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

### TCP 4043: Remote pairing software download

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4045: Remote pairing version information

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4047: Remote pairing session connection

The port is only available (and open) when a Touch panel is remote paired with the video conferencing device. You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4053: Remote pairing port

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 5060/5061: SIP listen ports

The SIP listen ports are open by default. The SIP listen ports are disabled by the Cisco UCM (Unified Communication Manager). You can close the ports by setting the SIP listen ports to **Off**.

```
SIP ListenPort: Off/On
```

### TCP 65533: Alternate port for Proximity connections

The port is closed by default. The port is open for Proximity connections when the setting to enable an alternate port for Proximity is set to **True**.

```
Proximity AlternatePort Enabled: False/True
```

The device settings are configured from the [Setup > Configuration](#) page on the web interface. Open a web browser and enter the IP address of the device then sign in.



## HTTPFeedback address from TMS

When a device is added to Cisco TelePresence Management Suite (TMS), it is automatically configured to send information (events) back to TMS. The device receives the address, that these events should be sent to, from TMS (HTTPFeedback address). If this address is absent or misconfigured, the device cannot send events to TMS.

### Missing response to events

If the device does not receive a response to an event, it will retry sending it to the HTTPFeedback address up to 6 times at increasing intervals.

If the device does not receive a response to any of the retries, the endpoint tries to send a message to the HTTPFeedback address every ten minutes. The HTTPFeedback status will indicate that it has failed, and there is a diagnostic message indicating the type of failure.

While retrying to send messages, there will be a loss of Call Detail Records (CDR) on TMS.

### Get a new HTTPFeedback address from TMS

In order to get a new address to send events to, you must restart the device and wait for the next management address push from TMS (scheduled or triggered by the TMS administrator).

## Link an on-premises registered device to Cisco Webex Edge for Devices

Devices running CE9.10 are ready for *Webex Edge for Devices*. You need the Device Connector tool in order to link the device to the Webex Edge. Read the Release Notes and *Webex Edge for Devices* article on Webex Help Center to find out when the tool is available.

You can use *Webex Edge for Devices* to link your on-premises registered devices to the Webex cloud service. This gives you access to select cloud features, while your registration, device configuration management, calling, and media services remain on-premises. You can manage the cloud services and get device diagnostics in Webex Control Hub.

### Set-up

We recommend that you register the device to the on-premises service first; then you link it to the Webex Edge. For information how to link a device to *Webex Edge for Devices*, read the Webex Edge for Devices article on [Webex Help Center](#).

### Features

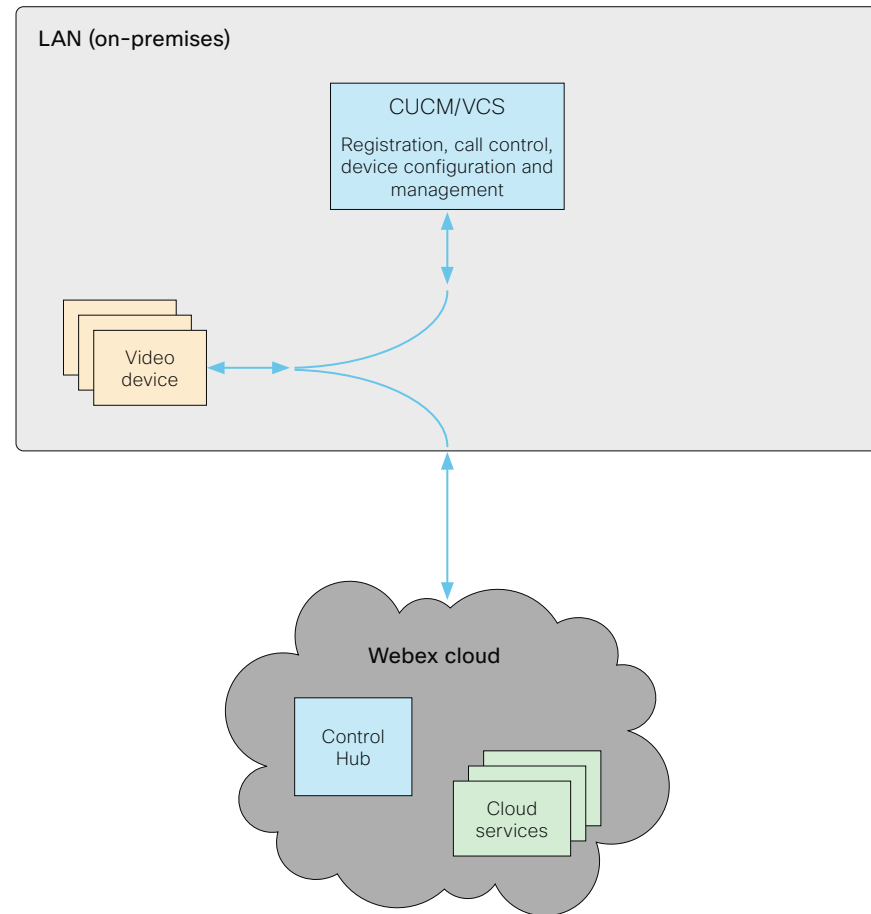
*Webex Edge for Devices* has the following features and functionality:

- Online/Offline connection status in Control Hub
- Device diagnostics with the ability to set administrator alerts
- Device historical analytics available directly in Control Hub
- Cloud xAPI access
- Hybrid calendar through Control Hub

The *Webex Edge for Devices* article referenced above has an updated list of all available features and limitations.

### Prerequisites

- Software version CE9.10 or later
- CUCM version 12.5su1, or 11.5.x with the latest device pack
- Control Hub administrator access
- Device Connector tool (to set up the link to Webex Edge)
- A cloud services license (Cisco Collaboration Flex Plan)



## Register a device to the Cisco Webex cloud service

You can register a device to Cisco Webex remotely from the web interface instead of using the on-screen setup assistant.

To register a device, you need to create an activation code on Control Hub first. To learn how to create an activation code, see [▶ Create a Place and Add Services for a Cisco Webex Room Device or a Cisco Webex Board](#)

From the web interface, you can only register a device that is not currently registered to a service.

**NOTE:** All local users and any customizations that have been created for this device will be deactivated.

1. Sign in to the web interface, and click [Click here to register to Webex](#) on the Home screen.

This link is only available if the device is not registered to a service already.

2. A pop-up appears and you can enter the activation code you have created on Control Hub.

Format:

- xxxx-xxxx-xxxx-xxxx, or
- xxxxxxxxxxxxxxxx

3. After registration, you must setup the time zone and language settings from the on-screen setup assistant. If the wizard times out, default settings will be applied.

### Limitations

Some of the available configurations only apply to on-premises registered devices. They don't apply to Webex registered devices. In the API guide's *Supported Commands Matrix*, these items are marked with "On-prem only".

Among the non-applicable configurations, are those related to H.323, H.320, SIP, NTP, CUCM, LDAP, Proximity, and Far End Camera Control.

### System Information

General		H323	
Product:	Cisco ...	Status	Inactive
System time:	12:30	Gatekeeper	-
Browser time:	12:30	Number	-
Last boot:	yesterday at 15:00	ID	-
Serial number:		<b>SIP</b>	
Software version:	ce...	Status	Inactive
Installed options:	Encryption RemoteMonitoring	Proxy	-
System name:	MySystem	<p><b>This video system is not registered</b></p> <p>In order to place calls with this video system, it needs to be registered to a call service.</p> <p><a href="#">Click here to register to Webex</a></p>	
IPv4:			
IPv6:			
MAC address:			
Temperature:	65.7°C / 150.3°F		

## 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).

CE software supports a range of RFCs, including the following:

- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3263 Locating SIP Servers
- RFC 3361 DHCP Option for SIP Servers
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- 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 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 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

## Technical specification (page 1 of 2)

### SOFTWARE COMPATIBILITY

- Cisco Collaboration Endpoint Software Version 9.1 or later
- RoomOS

### COMPONENTS

- Cisco Webex Room Kit Plus with Cisco Webex Codec Plus and Cisco Quad Camera
- Cisco Webex Room Kit Plus P60 with Cisco Webex Codec Plus and Cisco TelePresence Precision 60 camera

### BANDWIDTH

- Up to 6Mbps point-to-point

### MINIMUM BANDWIDTH FOR RESOLUTION / FRAME RATE

- H.264
  - 720p30 from 768 kbps
  - 720p60 from 1152 kbps
  - 1080p30 from 1472 kbps
  - 1080p60 from 2560 kbps

### FIREWALL TRAVERSAL

- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal

### VIDEO STANDARDS

- H.264
- H.265 (SIP)

### VIDEO INPUTS

- One HDMI input supports formats up to maximum 1080p60
- Two HDMI input<sup>\*</sup>, which supports formats up to maximum 3840 × 2160 at 30fps, including 1920 × 1080 at 60 fps
- Consumer Electronics Control (CEC) 2.0

### VIDEO OUTPUTS

- Two HDMI outputs<sup>\*</sup>, which support formats up to 3840 × 2160 at 60fps (4Kp60)
- Live video resolutions (encode and decode) up to 1920 × 1080 at 30fps or 60fps (HD1080p)
- Consumer Electronics Control (CEC) 2.0

### AUDIO STANDARDS

- AAC-LD
- G.722
- G.722.1
- G.711
- G.729
- Opus

### AUDIO FEATURES

- High quality 20kHz audio
- Prepared for subwoofer (line out)
- Prepared for inductive loop (line out)
- Automatic gain control (AGC)
- Automatic noise reduction
- Active lip synchronization

### AUDIO INPUTS

- Three microphones, 4-pole mini-jack
- Two audio in from HDMI

### AUDIO OUTPUTS (external)

- One line out mini-jack (stereo) (Codec Plus)
- One RCA output for subwoofer (Quad Camera)
- One HDMI output with audio, 48kHz, 24 bit, 2 channels (Codec Plus)
- Audio Return Channel (ARC) on one HDMI input (audio from Codec Plus to Quad Camera)

### LOUDSPEAKERS (internal), only applies to Room Kit Plus (Codec Plus + Quad Camera bundle)

- High-quality speakers
- Frequency response: 70 Hz to 20 kHz
- Max output level 90dB SPL

### SPEAKER TRACKING

- 6-element microphone array for speaker tracking

### DUAL STREAM

- H.239 dual stream (H.323)
- BFCP dual stream (SIP)
- Support for resolutions up to 3840 × 2160 at 8 fps; up to 1920 × 1080 at 30 fps

### WIRELESS SHARING

- Cisco Webex client (up to 3840 × 2160 at 5fps)
- Cisco Intelligent Proximity client (up to 1920 × 1080 at 5fps)

### MULTIPOINT SUPPORT

- Four-way embedded SIP/H.323 conferencing capability with MultiSite option

### MULTISITE FEATURES (EMBEDDED MULTIPOINT), optional upgrade

- Adaptive SIP/H.323 MultiSite:
  - Three-way resolution up to 1920 × 1080 at 30 fps, and content up to 3840 × 2160 at 5fps
  - Four-way resolution up to 1280 × 720 at 30 fps, and content up to 3840 × 2160 at 5fps
- Full individual audio and video transcoding
- H.323, SIP, and VoIP in the same conference
- Support for presentation (H.239/BFCP) from any participant at resolutions up to 3840 × 2160 at 5fps
- Best Impression (automatic continuous presence layouts)
- Encryption and dual stream from any site

### PROTOCOLS

- H.323
- SIP
- Cisco Webex

### EMBEDDED ENCRYPTION

- H.323 and SIP point-to-point
- Standards-based: H.235 v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange

### IP NETWORK FEATURES

- DNS lookup for service configuration
- Differentiated services (QoS)
- IP adaptive bandwidth management (including flow control)
- Automatic gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 DTMF tones in H.323
- RFC 4733 DTMF tones in SIP
- Date and time support using NTP
- Packet loss based downspeeding
- URI dialing
- DHCP (Dynamic Host Configuration Protocol)
- IEEE 802.1x network authentication
- IEEE 802.1q VLAN
- IEEE 802.1p QoS and class of service (CoS)
- ClearPath

### IPV6 NETWORK SUPPORT

- Single call stack support for both H.323 and SIP
- Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS and DiffServ
- Support for static IP address assignment, stateless autoconfiguration, and DHCPv6

### CISCO UNIFIED COMMUNICATIONS MANAGER

- Native registration with Cisco Unified Communications Manager (CUCM)
- Requires CUCM version 9.1.2 or later with device pack for Room Kit

### SUPPORTED INFRASTRUCTURE

- Cisco TelePresence Video Communication Server (Cisco VCS)

### SECURITY FEATURES

- Management using HTTPS and SSH
- IP administration password
- Administration menu password
- Disable IP services
- Network settings protection

<sup>\*</sup> HDMI version 1.4b for the input, HDMI version 2.0 for the outputs

## Technical specification (page 2 of 2)

### NETWORK INTERFACES

- One Ethernet (RJ-45) 10/100/1000 for LAN
- One Ethernet (RJ-45) 10/100/1000 for direct pairing with camera
- One Ethernet (RJ-45) 10/100/1000 with Power over Ethernet (PoE) for direct pairing with Touch 10
- Wi-Fi 802.11a/b/g/n/ac 2.4 GHz / 5 GHz for LAN. 2x2 MIMO

### OTHER INTERFACES

- USB 2.0 port
- Micro USB
- Factory reset pinhole

### CISCO QUAD CAMERA

- 5K Ultra HD camera
- Support up to 60 fps
- 15.1 MP image sensor
- 1/1.7 CMOS
- 5x digital zoom (3 tele-lenses, each with 50° horizontal field of view)
- f/2.0 aperture
- 83° horizontal field of view
- 51.5° vertical field of view
- Auto-framing (audio + face detect)
- 5120 × 2880 pixel resolution
- Auto focus, brightness, and white balance
- Focus distance 1 m to infinity

### CISCO TELEPRESENCE PRECISION 60 CAMERA

- 10 x optical zoom
- 2 x digital zoom
- 20 x total zoom
- Motorized +20°/-20° tilt
- Motorized ± 100° pan
- 48.8° vertical field of view
- 80° horizontal field of view
- F 1.5
- Focus distance 1 m - infinity (wide)
- 1920 × 1080 pixels at 60 fps
- Automatic or manual focus, brightness and white balance
- Ethernet camera control, (RJ-45) 10/100 Mbit
- Far-end camera control
- HDMI 1.4 and 3G-SDI output, and Daisy chain
- Upside-down mounting with automatic flipping of picture

### POWER

- Two power supplies
- 100-240VAC, 50/60Hz, 12V DC input
- Average 20W, peak 70W

### OPERATING TEMPERATURE AND HUMIDITY

- Ambient temperature: 0°C to 40°C (32°F to 104°F)
- Relative humidity (RH): 10% to 90%

### STORAGE AND TRANSPORT TEMPERATURE

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

### LOCKING MECHANISM

- Kensington security lock

### DIMENSIONS

- Width: 35.9mm / 14.1 in.
- Height: 4.3mm / 1.7 in.
- Depth: 14.3mm / 5.6 in.
- Weight: 1.77 kg / 3.9 lbs

### APPROVALS AND COMPLIANCE

- Directive 2014/35/EU (Low-Voltage Directive)
- Directive 2014/30/EU (EMC Directive) – Class A
- Directive 2014/53/EU (Radio Equipment Directive)
- Directive 2011/65/EU (RoHS)
- Directive 2002/96/EC (WEEE)
- NRTL approved (Product Safety)
- FCC CFR 47 Part 15B (EMC) – Class A
- FCC Listed (Radio Equipment)

Please check the Product Approval Status Database at <http://www.cisco.com> for approval documents per country.

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.

November 2019

## User documentation on the Cisco web site

Use the following short-links to find the documentation for the product series running CE software.

### Room Series:

▶ <https://www.cisco.com/go/room-docs>

### MX Series:

▶ <https://www.cisco.com/go/mx-docs>

### SX Series:

▶ <https://www.cisco.com/go/sx-docs>

### DX Series:

▶ <https://www.cisco.com/go/dx-docs>

### Boards:

▶ <https://www.cisco.com/go/board-docs>

In general, you can find user documentation for all Cisco Collaboration endpoints at ▶ <https://www.cisco.com/go/telepresence/docs>

The documents are organized in the following categories – some documents are not available for all products:

### Install and Upgrade > Install and Upgrade Guides

- *Installation guides*: How to install the product
- *Getting started guide*: Initial configurations required to get the device 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 device 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 device with the Cisco Unified Communications Manager (CUCM)
- *Spare parts overview, Spare parts replacement guides, Cable schemas*: Useful information when replacing spare parts

### Maintain and Operate > End-User Guides

- *User guides*: How to use the product
- *Quick reference guides*: How to use the product
- *Physical interface guide*: Details about the codec's physical interface, including the connector panel and LEDs

### Reference Guides > Command references

- *API reference guides*: Reference guide for the Application Programmer Interface (API)

### Reference Guides > Technical References

- *CAD drawings*: 2D CAD drawings with dimensions.

### Configure > Configuration Guides

- *Customization guide*: How to customize the user interface, how to use the device's API to program in-room controls, making macros, configure advanced audio set-ups using the Audio Console, and other customizations.

### 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: ► <https://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>.