Administrator guide

for Cisco Webex Room Kit Mini
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

**Introduction** .................................................................................................................. 5
- User documentation and software .............................................................................. 6
- What's new in CE9 ....................................................................................................... 7
- Room Kit Mini at a glance ........................................................................................... 17
- Power On and Off ......................................................................................................... 18
- LED indicators ............................................................................................................. 19
- How to administer the video conferencing device ....................................................... 20

**Configuration** ............................................................................................................ 24
- User administration .................................................................................................. 25
- Change the device passphrase ................................................................................... 26
- Restrict the access to the Settings menu .................................................................. 27
- Device configuration ................................................................................................ 28
- Add a sign in banner .................................................................................................. 29
- Add a welcome banner ............................................................................................. 30
- Manage the service certificates of the device ............................................................ 31
- Manage the lists of trusted certificate authorities - CAs ........................................... 32
- Set up secure audit logging ....................................................................................... 36
- Delete CUCM trust lists .............................................................................................. 37
- Change the persistency mode ..................................................................................... 38
- Set strong security mode ........................................................................................... 39
- Set up ad hoc multipoint conferences ....................................................................... 40
- Set up Intelligent Proximity for content sharing ......................................................... 42
- Adjust the video quality to call rate ratio ................................................................... 47
- Add corporate branding to the screen and Touch 10 user interface ............................ 49
- Add a custom wallpaper ............................................................................................. 51
- Choose a ringtone and set the ringtone volume ......................................................... 52
- Manage the Favorites list ........................................................................................... 53
- Set up accessibility features ....................................................................................... 54
- Provisioning of product specific configurations from CUCM .................................... 55

**Peripherals** .................................................................................................................. 57
- Connect a monitor ....................................................................................................... 58
- Connect an input source ............................................................................................. 59
- Extend the number of input sources ........................................................................... 61
- Information about displays ......................................................................................... 62
- Information about 4K resolution ............................................................................... 63
- Information about HDMI cables .................................................................................. 64
Set up the Best overview feature ................................................................. 65
Connect the Touch 10 controller ................................................................. 66
Connect the ISDN Link ............................................................................... 70
Maintenance ............................................................................................ 71
Upgrade the device software ...................................................................... 72
Add option keys ....................................................................................... 73
Device status ............................................................................................ 74
Run diagnostics ....................................................................................... 75
Download log files .................................................................................... 76
Create a remote support user .................................................................... 77
Backup and restore configurations and custom elements ......................... 78
CUCM provisioning of custom elements .................................................... 79
TMS provisioning of custom elements ....................................................... 80
Revert to the previously used software image ......................................... 81
Factory reset the video conferencing device ............................................. 82
Factory reset Cisco Touch 10 ....................................................................... 85
Factory reset Cisco TelePresence Touch 10 ................................................ 86
Capture user interface screenshots ........................................................... 87
Device settings ......................................................................................... 88
Overview of the device settings ................................................................ 89
Audio settings .......................................................................................... 94
CallHistory settings .................................................................................. 96
Cameras settings ...................................................................................... 97
Conference settings .................................................................................. 98
FacilityService settings ............................................................................ 103
H323 settings ........................................................................................... 104
Httpclient settings ................................................................................... 107
HttpFeedBack settings ............................................................................. 108
Logging settings ....................................................................................... 109
Macros settings ........................................................................................ 111
Network settings ...................................................................................... 112
NetworkServices settings ........................................................................ 120
Peripherals settings .................................................................................. 127
Phonebook settings .................................................................................. 129
Provisioning settings ............................................................................... 131
Proximity settings .................................................................................... 134
RoomAnalytics settings ............................................................................ 136
RoomReset settings ................................................................................. 137
RTP settings ............................................................................................. 138
Security settings ........................................................................................ 139
SerialPort settings .................................................................................... 142
SIP settings ............................................................................................... 143
Standby settings ....................................................................................... 148
SystemUnit settings .................................................................................. 150
Time settings ............................................................................................. 151
UserInterface settings ............................................................................... 154
UserManagement settings ......................................................................... 160
Video settings ........................................................................................... 164
WebEngine settings ................................................................................... 173
Experimental settings ............................................................................... 174
Appendices ............................................................................................... 175
How to use Touch 10 ............................................................................... 176
Using Room Kit Mini as a USB camera .................................................... 177
Set up remote monitoring .......................................................................... 178
Access call information and answer a call while using the web interface .... 179
Place a call using the web interface ........................................................... 180
Share content using the web interface ......................................................... 182
Local layout control .................................................................................. 183
Control a local camera ............................................................................. 184
Control a far end camera ........................................................................... 185
Packet loss resilience – ClearPath .............................................................. 186
Room analytics .......................................................................................... 187
Customize the video conferencing device’s Touch 10 user interface ......... 189
Customize the video conferencing device’s behavior using macros ......... 191
Remove default buttons from the user interface ........................................ 192
Use of a third-party USB input device ....................................................... 193
Sending HTTP(S) requests ...................................................................... 194
Digital signage .......................................................................................... 195
API-driven web views ............................................................................... 196
Input source composition .......................................................................... 197
Presentation source composition ............................................................... 199
Manage startup scripts ............................................................................ 201
Access the device’s XML files ................................................................... 202
Execute API commands and configurations from the web interface ......... 203
Connector panel ......................................................................................... 204
About Ethernet ports ................................................................................. 205
Serial interface for maintenance ............................................................... 206
Open TCP Ports ........................................................................................ 207
HTTP Feedback address from TMS ................................................................. 208
Link an on-premises registered device to Cisco Webex Edge for Devices .......... 209
Register a device to the Cisco Webex cloud service ........................................ 210
Supported RFCs ............................................................................... 211
Technical specification ....................................................................... 212
User documentation on the Cisco web site ............................................... 214
Cisco contacts ........................................................................... 215
Chapter 1

Introduction
User documentation and software

Products covered in this guide

- Cisco Webex Room Kit Mini

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):

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 CE9.6.

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:


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

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 550, 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 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

- 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

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
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
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
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
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
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 programatically 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
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
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
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.

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)

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
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 PasswordPolicyReuseLimit (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 Kit Mini, 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: StartTls
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)
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
- 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
Room Kit Mini at a glance

Cisco Webex Room Kit Mini includes camera, codec, speakers, and microphones that integrates with 4K screen. It is easy to mount and integrates well with flat panel displays through HDMI CEC.

The Room Kit Mini is designed for huddle spaces with three to five people because of its wide 120-degree field of view. It brings sophisticated features, which were previously the domain of higher-end video conferencing rooms, to every room and every team.

The Room Kit Mini is built for both cloud (Cisco Webex) and on-premises (CUCM and VCS) deployments.

Features and benefits

- Discreet, integrated camera with intelligent view capabilities: detects meeting participants and shows the best overview
- Counts people in the room, enabling analytics for better resource planning
- Integrated microphones and loudspeakers provide a great audio experience
- Automatic noise suppression, reducing disruptive sounds coming from the meeting room
- Automatic wake-up feature that detects when someone walks into the room and recognize them through their mobile device
- Controlled by the Cisco Touch 10 or with a Cisco Webex Teams app
- Controls peripherals such as lights and blinds through the Cisco Touch 10 (in-room control)
- 4K content sharing (30 fps in local meetings; 5 fps when sharing with far-end)
- Wired or wireless content sharing
- Ethernet and Wi-Fi
- USB camera mode (including the video conferencing device’s camera, microphones, and loudspeakers)
- You can find more information about the Cisco Webex Room Kit Mini at https://www.cisco.com/go/roomkit
Power On and Off

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, you have to disconnect the power plug and connect it again.
LED indicators

System LED

*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.

Camera LED

*Incoming call:*
  - The LED flashes.

*In call:*
  - Steady light.

*Selfview on:*
  - Steady light.
How to administer the video conferencing device

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.

<table>
<thead>
<tr>
<th>Access method</th>
<th>Notes</th>
<th>How to enable/disable the methods</th>
</tr>
</thead>
</table>
| HTTP/HTTPS    | • Used by the web interface of the device  
• Non-secure (HTTP) or secure (HTTPS) communication  
• HTTPS: Enabled by default  
• HTTP: Enabled 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 | NetworkServices > HTTP > Mode  
Restart the device for changes to take effect |
| WebSocket      | • Tied to HTTP, so that also HTTP or HTTPS must be enabled before you can use WebSocket  
• Encrypted (wss) or unencrypted (ws) communication  
• Disabled by default | NetworkServices > HTTP > Mode  
NetworkServices > Websocket  
Restart the device for changes to take effect |
| SSH           | • Secure TCP/IP connection  
• Enabled by default | NetworkServices > SSH > Mode  
You do not need to restart the device. It may take some time for changes to take effect |
| Serial connection | • Connect to the device with a cable. IP-address, DNS, or a network is not required  
• Enabled by default  
• For security reasons, you are asked to sign in by default ($SerialPort > LoginRequired$) | SerialPort > Mode  
Restart the device for changes to take effect |

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.
The web interface of the device

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

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
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 3rd 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.
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 setting'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.

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 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.
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 kB

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

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.
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.

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.

View or disable certificates

Use the Details... and Disable buttons respectively, to view or disable certificates.

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

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.
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.

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.

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.
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

The custom list of trusted CA certificates 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.

1. Open the Security category.
2. Find the Audit > Server settings, and enter the Address of the audit server. If you set Port Assignment 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 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.

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 trace back 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.

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  

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) ¹.

![Centralized conference infrastructure diagram]

In this set-up video devices A, B, C and D participate 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.

![Local conference resources diagram]

In this set-up video devices A, B, C and D participate 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)

¹ MCU - multipoint control unit, also called video-conferencing gateway or bridge.
Set up ad hoc multipoint conferences  (page 2 of 2)

<table>
<thead>
<tr>
<th>Conference Multipoint Mode setting</th>
<th>MultiSite option key</th>
<th>Remote device type</th>
<th>Add participant behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off 3</td>
<td>N/A</td>
<td>MCU</td>
<td>Direct Remote Add</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Video device</td>
<td>Plus one audio</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCU Direct Remote Add</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CUCM-MediaResource-GroupList</td>
<td>N/A</td>
<td>Video device</td>
<td>Consultative Add</td>
</tr>
<tr>
<td>MultiSite 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>N/A</td>
<td>Local Multisite</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Plus one audio</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto</td>
<td>MCU</td>
<td>Direct Remote Add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video device</td>
<td>Local Multisite</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>without cascading</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>MCU</td>
<td>Direct Remote Add</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video device</td>
<td>Plus one audio</td>
<td></td>
</tr>
</tbody>
</table>

- If the MCU supports Add Participant, there is an Add 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.
- If the MCU does not support Add Participant, there is no Add button in the UI.
- You can keep adding participants until you reach the maximum number for the device.
- Only the MultiSite host (which is now acting as an MCU) can add participants. This prevents cascaded conferences.

- Available only to CUCM registered devices, and the SIP Type setting must be Cisco.
- 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.
- Only the participant who added the first new participant to the conference can add more participants.

4 We recommend setting Conference Multipoint Mode to Auto rather than to MultiSite in order to avoid cascaded conferences.

---

2 The remote device type is shown in the Call [n] DeviceType status.
3 Not supported for SX10, DX70, and DX80.
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

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

* 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

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.

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.
Enable Proximity services

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

2. Go to Proximity > Mode. Check that Proximity is On (default), so that the video conferencing device sends 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 On by default.

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.
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
- 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).
Adjust the video quality to call rate ratio

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.

Allowing video at 60 fps

As default, the camera outputs 30 frames per second (fps). This allows for good quality both in close-ups and overview pictures for normal bandwidths and lighting conditions. If the conditions are better, a 60 fps output from the camera may give a better overall quality.

Use the Cameras Camera Framerate setting to set the camera output framerate.
### 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

<table>
<thead>
<tr>
<th>Call rate [kbps]</th>
<th>H.264, maximum 30fps</th>
<th></th>
<th>H.264, maximum 60fps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>Medium</td>
<td>High</td>
<td>Normal</td>
</tr>
<tr>
<td>128</td>
<td>320×180@30</td>
<td>320×180@30</td>
<td>512×288@30</td>
<td>320×180@30</td>
</tr>
<tr>
<td>256</td>
<td>512×288@30</td>
<td>640×360@30</td>
<td>768×448@30</td>
<td>512×288@30</td>
</tr>
<tr>
<td>384</td>
<td>640×360@30</td>
<td>768×448@30</td>
<td>768×448@30</td>
<td>640×360@30</td>
</tr>
<tr>
<td>512</td>
<td>768x448@30</td>
<td>1024x576@30</td>
<td>1024x576@30</td>
<td>768x448@30</td>
</tr>
<tr>
<td>768</td>
<td>1024×576@30</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
<td>1024×576@30</td>
</tr>
<tr>
<td>1152</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>1472</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>1920</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>2560</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>3072</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>4000</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>6000</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Call rate [kbps]</th>
<th>H.265, maximum 30fps</th>
<th></th>
<th>H.265, maximum 60fps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>Medium</td>
<td>High</td>
<td>Normal</td>
</tr>
<tr>
<td>128</td>
<td>512×288@30</td>
<td>512×288@30</td>
<td>640×360@30</td>
<td>512×288@30</td>
</tr>
<tr>
<td>256</td>
<td>640×360@30</td>
<td>768×448@30</td>
<td>768×448@30</td>
<td>640×360@30</td>
</tr>
<tr>
<td>384</td>
<td>768×448@30</td>
<td>1024×576@30</td>
<td>1280×720@30</td>
<td>768×448@30</td>
</tr>
<tr>
<td>512</td>
<td>1024×576@30</td>
<td>1280×720@30</td>
<td>1280×720@30</td>
<td>1024×576@30</td>
</tr>
<tr>
<td>768</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>1152</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>1472</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>1920</td>
<td>1280×720@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>2560</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>3072</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>4000</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
<tr>
<td>6000</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1920×1080@30</td>
<td>1280×720@30</td>
</tr>
</tbody>
</table>
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)

About Branding
The Branding feature, as described 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.

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 272×272 pixels (it will be scaled automatically)
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 choosen 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.
3. Choose a folder in the folder drop down list in order to store the contact in a sub-folder.
4. 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).
5. 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.
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.
Chapter 3

Peripherals
Connect a monitor

The device has one HDMI video output. The HDMI output support resolutions up to 3840 × 2160 at 60fps. You need Premium HDMI cables to support the high resolutions and frame rates. There isn’t audio on the HDMI outputs.

⚠️ Always switch off power when you connect and disconnect monitors and other peripherals.
Connect an input source (page 1 of 2)

Sign in to the web interface and navigate to Setup > Configuration, to find the settings referred below.

Connect a computer or other content source

You can connect one input source, for example a computer, to the device’s HDMI input (Input Connector 2) in order to share content locally or with conference participants.

The HDMI input supports resolutions up to 3840 × 2160 at 30 fps. You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates.
Connect an input source  (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.

Note that Input Connector 1 is the integrated camera.

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 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 Sharpness for Connector 2.
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.

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.

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
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.

<table>
<thead>
<tr>
<th>Model</th>
<th>LG global website link</th>
</tr>
</thead>
<tbody>
<tr>
<td>49&quot; UHD (49UH5C)</td>
<td><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></td>
</tr>
<tr>
<td>55&quot; UHD (55UH5C)</td>
<td><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></td>
</tr>
<tr>
<td>65&quot; UHD (65UH5C)</td>
<td><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></td>
</tr>
<tr>
<td>75&quot; UHD (75UH5C)</td>
<td><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></td>
</tr>
<tr>
<td>86&quot; UHD (86UH5C)</td>
<td><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></td>
</tr>
<tr>
<td>98&quot; UHD (98UH5C)</td>
<td><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></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model</th>
<th>Samsung global website link</th>
</tr>
</thead>
<tbody>
<tr>
<td>QMN Series</td>
<td><a href="https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N">https://displaysolutions.samsung.com/digital-signage/detail/1269/QM43N</a></td>
</tr>
<tr>
<td>QBN Series</td>
<td><a href="https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N">https://displaysolutions.samsung.com/digital-signage/detail/1274/QB43N</a></td>
</tr>
</tbody>
</table>
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).

* 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.

You can find more information about HDMI cables at [http://www.hdmi.org](http://www.hdmi.org)
Set up the Best overview feature

Sign in to the web interface and navigate to **Setup > Configuration**, to find the settings referred.

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

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 enter the room, the feature will adopt to the changes and automatically adjust the view to include all persons in the picture.

Configure Best overview

Use the **Cameras > SpeakerTrack** settings to configure best overview.

**Cameras > SpeakerTrack > Mode**

- **Auto**: Best overview is enabled in general. The device will detect people in the room and automatically select the best camera framing. Users can switch Best overview on or off instantly in the camera control panel on the Touch controller.
- **Off**: Best overview is switched off, and it is not possible to switch it on from the user interface.
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 paring 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 paring 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.

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.

- Touch screen
- Sound bar for audio adjustment
- Audio mute
- Adjustable support to accommodate individual ergonomic needs
- Two USB connectors (not in use)
- Mini-jack, 3.5 mm (not in use)
- Micro-USB: for maintenance only
- Ethernet with PoE: for power and Ethernet
- Not in use
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 supports 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 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


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-yyyy.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).

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.
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.

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.

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.

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


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

Create remote support user

1. Click Create user.
2. Open a case with Cisco TAC.
3. Copy the text in the Token field and send it to Cisco TAC.
4. Cisco TAC will generate a password.
   The remote support user is valid for seven days, or until it is deleted.

Delete remote support user

Click Delete user.

About the remote support user

In cases where you need to diagnose problems on the 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
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:

   ```xml
   <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.

   * 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.

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.
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.
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.
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. Tilt the unit forward to find the reset button (pin hole).

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.
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

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 [x] 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 known 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.

Audio settings

- Audio DefaultVolume
- Audio Input HDMI [n] Level
- Audio Input HDMI [n] Mode
- Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo
- Audio KeyClickDetector Attenuate
- Audio KeyClickDetector Enabled
- Audio Microphones Mute Enabled
- Audio SoundsAndAlerts RingTone
- Audio SoundsAndAlerts RingVolume
- Audio Ultrasound MaxVolume
- Audio Ultrasound Mode

CallHistory settings

- CallHistory Mode

Cameras settings

- Cameras Camera Framerate
- Cameras PowerLine Frequency
- Cameras SpeakerTrack Mode

Conference settings

- Conference ActiveControl Mode
- Conference AutoAnswer Delay
- Conference AutoAnswer Mode
- Conference AutoAnswer Mute
- Conference CallProtocolIPStack
- Conference DefaultCall Protocol
- Conference DefaultCall Rate
- Conference DoNotDisturb DefaultTimeout
- Conference Encryption Mode
- Conference FarEndControl Mode
- Conference FarEndControl SignalCapability
- Conference FarEndMessage Mode
- Conference IncomingMultisiteCall Mode
- Conference MaxReceiveCallRate
- Conference MaxTotalReceiveCallRate
- Conference MaxTotalTransmitCallRate
Conference MaxTransmitCallRate .......................................................... 100
Conference MicUnmuteOnDisconnect Mode ....................................... 101
Conference Multipoint Mode .............................................................. 101
Conference MultiStream Mode ........................................................... 102
Conference Presentation OnPlacedOnHold .......................................... 102
Conference Presentation RelayQuality ............................................... 102
Conference VideoBandwidth Mode ...................................................... 102

FacilityService settings .................................................................... 103
FacilityService Service \([n]\) CallType ......................................................... 103
FacilityService Service \([n]\) Name .......................................................... 103
FacilityService Service \([n]\) Number ....................................................... 103
FacilityService Service \([n]\) Type .......................................................... 103

H323 settings ...................................................................................... 104
H323 Authentication LoginName .......................................................... 104
H323 Authentication Mode ................................................................. 104
H323 Authentication Password ........................................................... 104
H323 CallSetup Mode ......................................................................... 104
H323 Encryption KeySize ................................................................. 105
H323 Gatekeeper Address ................................................................... 105
H323 H323Alias E164 ......................................................................... 105
H323 H323Alias ID ............................................................................. 105
H323 NAT Address .............................................................................. 106
H323 NAT Mode ................................................................................ 106
H323 PortAllocation ........................................................................... 106

HttpClient settings ........................................................................... 107
HttpClient AllowHTTP ........................................................................ 107
HttpClient AllowInsecureHTTPS ...................................................... 107
HttpClient Mode ............................................................................... 107

HttpFeedback settings ..................................................................... 108
HttpFeedback TlsVerify ....................................................................... 108

Logging settings ............................................................................... 109
Logging Debug Wifi ........................................................................... 109
Logging External Mode ....................................................................... 109
Logging External Protocol .................................................................. 109
Logging External Server Address ...................................................... 109
Logging External Server Port ............................................................ 109
Logging External TlsVerify ................................................................ 110
Logging Internal Mode ....................................................................... 110
Logging Mode ................................................................................... 110

Macros settings ................................................................................. 111
Macros AutoStart .............................................................................. 111
Macros Mode ..................................................................................... 111
Macros UnresponsiveTimeout .......................................................... 111
Macros XAPI Transport .................................................................... 111

Network settings .............................................................................. 112
Network \([n]\) DNS DNSSEC Mode ....................................................... 112
Network \([n]\) DNS Domain Name ........................................................ 112
Network \([n]\) DNS Server \([m]\) Address ................................................. 112
Network \([n]\) IEEE8021X AnonymousIdentity .................................... 113
Network \([n]\) IEEE8021X Eap Md5 ....................................................... 114
Network \([n]\) IEEE8021X Eap Peap ....................................................... 114
Network \([n]\) IEEE8021X Eap Ttls ....................................................... 114
Network \([n]\) IEEE8021X Eap Ttls ....................................................... 114
Network \([n]\) IEEE8021X Identity ......................................................... 113
Network \([n]\) IEEE8021X Mode ........................................................... 112
Network \([n]\) IEEE8021X Password .................................................... 113
Network \([n]\) IEEE8021X TlsVerify ..................................................... 113
Network \([n]\) IEEE8021X UseClientCertificate .................................. 113
Network \([n]\) IPStack ......................................................................... 114
Network \([n]\) IPv4 Address ................................................................. 115
Network \([n]\) IPv4 Assignment ........................................................... 115
Network \([n]\) IPv4 Gateway ............................................................... 115
Network \([n]\) IPv4 SubnetMask ........................................................... 115
Network \([n]\) IPv6 Address ................................................................. 116
Network \([n]\) IPv6 Assignment ........................................................... 115
Network \([n]\) IPv6 DHCPOptions ....................................................... 116
Network \([n]\) IPv6 Gateway ............................................................... 116
Network \([n]\) MTU ............................................................................... 116
Network \([n]\) QoS Diffserv Audio ....................................................... 117
Network \([n]\) QoS Diffserv Data .......................................................... 117
Network \([n]\) QoS Diffserv ICMPv6 .................................................... 118
Network \([n]\) QoS Diffserv NTP .......................................................... 118
Network \([n]\) QoS Diffserv Signalling .................................................. 117

Network \([n]\) QoS Diffserv Audio ....................................................... 117
Network \([n]\) QoS Diffserv Data .......................................................... 117
Network \([n]\) QoS Diffserv ICMPv6 .................................................... 118
Network \([n]\) QoS Diffserv NTP .......................................................... 118
Network \([n]\) QoS Diffserv Signalling .................................................. 117
NetworkServices settings ....................................................... 120
NetworkServices CDP Mode ............................................. 120
NetworkServices H323 Mode .............................................. 120
NetworkServices HTTP Mode ............................................ 120
NetworkServices HTTP Proxy LoginName ......................... 120
NetworkServices HTTP Proxy Mode .................................... 121
NetworkServices HTTP Proxy PACUrl ................................. 121
NetworkServices HTTP Proxy Password .............................. 121
NetworkServices HTTP Proxy URL ...................................... 121
NetworkServices HTTPS OCSP Mode ................................. 121
NetworkServices HTTPS OCSP URL .................................... 122
NetworkServices HTTPS Server MinimumTLSVersion ............ 122
NetworkServices HTTPS StrictTransportSecurity ................ 122
NetworkServices HTTPS VerifyClientCertificate .................. 122
NetworkServices NTP Mode .............................................. 122
NetworkServices NTP Server [n] Address .............................. 123
NetworkServices NTP Server [n] Key .................................... 123
NetworkServices NTP Server [n] KeyAlgorithm ..................... 123
NetworkServices NTP Server [n] KeyId ................................. 123
NetworkServices SIP Mode .............................................. 123
NetworkServices SNMP CommunityName ......................... 124
NetworkServices SNMP Host [n] Address ............................ 124
NetworkServices SNMP Mode ............................................ 123
NetworkServices SNMP SystemContact .............................. 124
NetworkServices SNMP SystemLocation ............................ 124
NetworkServices SSH AllowPublicKey ................................. 124
NetworkServices SSH HostKeyAlgorithm .............................. 124
NetworkServices SSH Mode .............................................. 124
NetworkServices UPhP Mode ............................................. 125
NetworkServices UPhP Timeout .......................................... 125

NetworkServices Websocket ............................................. 125
NetworkServices WelcomeText .......................................... 125
NetworkServices Wifi Allowed .......................................... 126
NetworkServices Wifi Enabled .......................................... 126
NetworkServices XMLAPI Mode ........................................ 126

Peripherals settings ......................................................... 127
Peripherals InputDevice Mode .......................................... 127
Peripherals Pairing CiscoTouchPanels EnableResilience ......... 127
Peripherals Pairing CiscoTouchPanels RemotePairing ............ 127
Peripherals Profile Cameras ............................................. 127
Peripherals Profile ControlSystems ................................. 128
Peripherals Profile TouchPanels ....................................... 128

Phonebook settings ......................................................... 129
Phonebook Server [n] ID .................................................. 129
Phonebook Server [n] Pagination ........................................ 129
Phonebook Server [n] TlsVerify ........................................ 129
Phonebook Server [n] Type .............................................. 130
Phonebook Server [n] URL .............................................. 130

Provisioning settings ...................................................... 131
Provisioning Connectivity .............................................. 131
Provisioning ExternalManager Address ............................... 131
Provisioning ExternalManager AlternateAddress ................ 131
Provisioning ExternalManager Domain .............................. 132
Provisioning ExternalManager Path ................................... 132
Provisioning ExternalManager Protocol ............................. 131
Provisioning LoginName ............................................... 132
Provisioning Mode ....................................................... 132
Provisioning Password ................................................ 133
Provisioning TlsVerify ................................................ 133
Provisioning WebexEdge .............................................. 133

Proximity settings ......................................................... 134
Proximity AlternatePort Enabled ...................................... 134
Proximity Mode ......................................................... 134
Proximity Services CallControl ........................................ 134
Proximity Services ContentShare FromClients .................... 135
Proximity Services ContentShare ToClients ....................... 135
RoomAnalytics settings ........................................................................................................... 136
RoomAnalytics AmbientNoiseEstimation Mode ................................................................. 136
RoomAnalytics PeopleCountOutOfCall .............................................................................. 136
RoomAnalytics PeoplePresenceDetector .............................................................................. 136

RoomReset settings ........................................................................................................... 137
RoomReset Control .............................................................................................................. 137

RTP settings ......................................................................................................................... 138
RTP Ports Range Start .......................................................................................................... 138
RTP Ports Range Stop ........................................................................................................... 138
RTP Video Ports Range Start .............................................................................................. 138
RTP Video Ports Range Stop ............................................................................................... 138

Security settings .................................................................................................................. 139
Security Audit Logging Mode .............................................................................................. 139
Security Audit OnError Action ............................................................................................ 139
Security Audit Server Address ............................................................................................ 139
Security Audit Server Port ................................................................................................... 139
Security Audit Server PortAssignment ................................................................................. 140
Security Fips Mode .............................................................................................................. 140
Security Session FailedLoginsLockoutTime ......................................................................... 140
Security Session InactivityTimeout ..................................................................................... 140
Security Session MaxFailedLogins ..................................................................................... 140
Security Session MaxSessionsPerUser ............................................................................... 141
Security Session MaxTotalSessions .................................................................................... 141
Security Session ShowLastLogon ........................................................................................ 141

SerialPort settings .............................................................................................................. 142
SerialPort BaudRate ............................................................................................................. 142
SerialPort LoginRequired ................................................................................................... 142
SerialPort Mode .................................................................................................................. 142

SIP settings .......................................................................................................................... 143
SIP ANAT .............................................................................................................................. 143
SIP Authentication Password ............................................................................................. 143
SIP Authentication UserName ............................................................................................... 143
SIP DefaultTransport .......................................................................................................... 143
SIP DisplayName .................................................................................................................. 143
SIP Ice DefaultCandidate .................................................................................................... 144
SIP Ice Mode ....................................................................................................................... 144
SIP Line ............................................................................................................................... 144

SIP ListenPort ....................................................................................................................... 144
SIP Mailbox .......................................................................................................................... 144
SIP MinimumTLSVersion .................................................................................................... 144
SIP PreferredIPSignaling ..................................................................................................... 144
SIP Proxy [n] Address ........................................................................................................ 144
SIP TlsVerify ....................................................................................................................... 144
SIP Turn DiscoverMode ..................................................................................................... 145
SIP Turn DropRfIx .............................................................................................................. 145
SIP Turn Password ............................................................................................................. 145
SIP Turn Server ................................................................................................................... 145
SIP Turn UserName ............................................................................................................. 145
SIP Type .............................................................................................................................. 145
SIP URI ............................................................................................................................... 145

Standby settings .................................................................................................................. 148
Standby BootAction ............................................................................................................ 148
Standby Control ................................................................................................................... 148
Standby Delay ..................................................................................................................... 148
Standby Signage Audio ...................................................................................................... 148
Standby Signage Mode ....................................................................................................... 148
Standby Signage RefreshInterval ....................................................................................... 148
Standby Signage Url .......................................................................................................... 148
Standby StandbyAction ...................................................................................................... 149
Standby WakeupAction ...................................................................................................... 149
Standby WakeupOnMotionDetection ............................................................................... 149

SystemUnit settings ............................................................................................................. 150
SystemUnit CrashReporting Advanced ............................................................................. 150
SystemUnit CrashReporting Mode ................................................................................... 150
SystemUnit CrashReporting Url ....................................................................................... 150
SystemUnit Name ............................................................................................................... 150

Time settings ....................................................................................................................... 151
Time DateFormat ................................................................................................................ 151
Time TimeFormat ................................................................................................................ 151
Time Zone ........................................................................................................................... 152

UserInterface settings ......................................................................................................... 154
UserInterface Accessibility IncomingCallNotification ....................................................... 154
UserInterface Assistant Mode ............................................................................................ 154
UserInterface Assistant Mode ............................................................................................ 154
UserInterface Branding AwakeBranding Colors ................................................................. 154
UserInterface ContactInfo Type ......................................................................................... 155
UserInterface CustomMessage .......................................................................................... 155
UserInterface Features Call End ....................................................................................... 155
UserInterface Features Call JoinWebex .......................................................................... 156
UserInterface Features Call MidCallControls ................................................................. 155
UserInterface Features Call Start ..................................................................................... 156
UserInterface Features Call VideoMidControls ............................................................... 156
UserInterface Features Share Start .................................................................................. 156
UserInterface KeyTones Mode .......................................................................................... 155
UserInterface Language .................................................................................................... 156
UserInterface OSD EncryptionIndicator ........................................................................ 157
UserInterface OSD HalfwakeMessage ............................................................................. 157
UserInterface OSD Output ................................................................................................ 157
UserInterface Phonebook Mode ....................................................................................... 157
UserInterface Security Mode ............................................................................................ 157
UserInterface SettingsMenu Mode .................................................................................... 158
UserInterface SettingsMenu Visibility ................................................................................ 158
UserInterface SoundEffects Mode .................................................................................... 158
UserInterface UsbPromotion ............................................................................................. 159
UserInterface Wallpaper .................................................................................................. 158
UserInterface WebcamOnlyMode ...................................................................................... 159

UserManagement settings................................................................................................. 160
UserManagement LDAP Admin Filter ............................................................................... 160
UserManagement LDAP Admin Group .......................................................................... 160
UserManagement LDAP Attribute .................................................................................. 160
UserManagement LDAP BaseDN ..................................................................................... 160
UserManagement LDAP Encryption ................................................................................ 160
UserManagement LDAP MinimumTLSVersion .............................................................. 161
UserManagement LDAP Mode ........................................................................................ 161
UserManagement LDAP Server Address ......................................................................... 161
UserManagement LDAP Server Port ................................................................................. 161
UserManagement LDAP VerifyServerCertificate .......................................................... 161
UserManagement PasswordPolicy Complexity MinimumDigits ..................................... 162
UserManagement PasswordPolicy Complexity MinimumLength .................................... 162
UserManagement PasswordPolicy Complexity MinimumLowercase ......................... 162
UserManagement PasswordPolicy Complexity MinimumSpecial ................................ 162

UserManagement PasswordPolicy Complexity MinimumUppercase ......................... 163
UserManagement PasswordPolicy MaxLifetime ............................................................ 163
UserManagement PasswordPolicy ReuseLimit ................................................................ 163

Video settings.................................................................................................................. 164
Video ActiveSpeaker DefaultPIPPosition ........................................................................ 164
Video DefaultLayoutFamily Local .................................................................................... 164
Video DefaultLayoutFamily Remote ................................................................................ 165
Video DefaultMainSource ............................................................................................... 165
Video Input Connector [n] CameraControl Camerald ...................................................... 165
Video Input Connector [n] CameraControl Mode ............................................................. 165
Video Input Connector [n] CEC Mode ................................................................................. 165
Video Input Connector [n] InputSourceType ..................................................................... 166
Video Input Connector [n] Name ....................................................................................... 166
Video Input Connector [n] OptimalDefinition Profile ...................................................... 166
Video Input Connector [n] OptimalDefinition Threshold60fps ...................................... 167
Video Input Connector [n] PreferredResolution ............................................................... 167
Video Input Connector [n] PresentationSelection ............................................................. 167
Video Input Connector [n] Quality .................................................................................... 168
Video Input Connector [n] RGBQuantizationRange ........................................................ 168
Video Input Connector [n] Visibility ............................................................................... 168
Video Output Connector [n] CEC Mode ............................................................................ 169
Video Output Connector [n] MonitorRole ......................................................................... 169
Video Output Connector [n] Resolution .......................................................................... 169
Video Output Connector [n] RGBQuantizationRange ...................................................... 170
Video Presentation DefaultPIPPosition ............................................................................ 170
Video Presentation DefaultSource .................................................................................. 170
Video Presentation Priority ............................................................................................ 170
Video Selfview Default FullscreenMode ........................................................................ 171
Video Selfview Default Mode ........................................................................................ 171
Video Selfview Default OnMonitorRole ......................................................................... 171
Video Selfview Default PIPPosition ................................................................................. 171
Video Selfview OnCall Duration ..................................................................................... 172
Video Selfview OnCall Mode ......................................................................................... 172

WebEngine settings......................................................................................................... 173
WebEngine Mode ............................................................................................................. 173
WebEngine RemoteDebugging ......................................................................................... 173

Experimental settings .................................................................................................... 174
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 HDMI [n] Level
n: 1..1
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: 1..1
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: 1..1
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 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 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/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..70)
  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 Framerate
As default, the camera outputs 30 frames per second. This allows for good quality both in close-ups and overview pictures for normal bandwidths and lighting conditions. If the conditions are better, a 60 frames per second output from the camera may give a better overall quality.

Requires user role: ADMIN
Default value: 30

Value space: 30/60
- 30: The camera outputs 30 frames per second.
- 60: The camera outputs 60 frames per second.

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 SpeakerTrack Mode
The video conferencing device supports the Best overview feature. Best overview uses automatic camera framing to select the best camera view based on where people are in the room. Speaker tracking is not supported.

Requires user role: ADMIN, INTEGRATOR
Default value: Auto

Value space: Auto/Off
- Auto: Best overview is switched on. The device will detect people in the room and automatically select the best camera framing. Users can switch best overview 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: Best overview is switched off.
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 transmit 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 Port Allocation

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

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

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 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

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

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

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

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

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

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 heartbeats 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: On
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 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.
Cisco Webex Room Kit Mini

Administrator Guide

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 Port Assignment

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.

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: On

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 IANA Time Zone Database.

Requires user role: ADMIN,TEGRATOR, 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/Casarablanca, 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/Argentina, America/Bahia, America/Bahia_Blanca, America/Belize, America/Blanco, 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/Coast_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepae, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Grace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayquil, 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/Iruvik, 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/Maciejo, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Monemee, America/Merida, America/Metaltakla, America/Mexico_City, America/Miquelon, America/Moncont, 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/Centur, America/North_Dakota/New_Salem, America/Ofinaga, America/Onaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Porto-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/Scorebysund, America/Shiprock, America/Sitka, America/St_Barthlemy, 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, Antartica/Carey, Antartica/Davis, Antartica/DumontDUrville, Antartica/Macquarie, Antartica/Mawson, Antartica/Mcmurdo, Antartica/Palmer, Antartica/Rothera, Antartica/South_Pole, Antartica/Syowa, Antartica/Troll, Antartica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Asghabat, Asia/Ashgabat, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Chobi, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Gazia, Asia/Harbin, Asia/Hebron, Asia/He_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Ifukuts, Asia/Istanbul, Asia/Iskenderun, Asia/Isfahan, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khanty, 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/Oural, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Reykjavik, Asia/Salinas, Asia/Salts, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Sri_Nakrolmysk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Toms, Asia/Uigur, Asia/Ulanbaatar, Asia/Ulan_Bator, Asia/Urumpi, Asia/Ushter, Asia/Vientiane, Asia/Vladivostok, Asia/Yakuts, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faroe, Atlantic/Iceland, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Cairns, 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/Edmonton, 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+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/

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.

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/Czeck/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.
User Interface 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.

User Interface 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.

User Interface 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
- Auto: The device sends the on-screen information and indicators to the device's screen.

User Interface 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.

User Interface 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 User Interface Settings Menu 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.
- Custom: There is no background image on the screen.
- None: 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.
User Interface `UsbPromotion`

Choose whether or not to show on the halfwake screen, a text that informs you that you can use the device as a USB camera.

Requires user role: ADMIN
Default value: Off

Value space: Off/On
- Off: The USB camera information text is not shown.
- On: The USB camera information text is shown.

User Interface `WebcamOnlyMode`

This device can be used as a web camera, and as a normal video conferencing device. It can be used as a web camera even if it is not registered to any on-premise or cloud call service (such as CUCM, VCS, and Webex).

This setting determines if the user interface shall be adapted to a web camera only scenario when the video conferencing device is not registered.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/Off
- Auto: If the device is registered to a call service, the full user interface will be shown. If the device is not registered, and therefore cannot be used for calling, irrelevant user interface elements are removed.
- Off: The device will always show the full user interface.
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 passwords. 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.
- CentreRight: 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
- The source that is used as the default main video source.

Video Input Connector [n] CameraControl CameraId n: 1..2
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: 1
Value space: Connector n: 1
- The camera ID is fixed and cannot be changed.

Video Input Connector [n] CameraControl Mode n: 1..2
Define whether the camera that is connected to this video input connector can be controlled or not.
Note that camera control is not available for Connector 2 (HDMI).

Requires user role: ADMIN, INTEGRATOR
Default value: Connector 1: On Connector 2: Off
Value space: Connector 1: Off/On Connector 2: Off
- Off: Disable camera control.
- On: Enable camera control.

Video Input Connector [n] CEC Mode n: 2..2
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.

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] InputSourceType

n: 1..2

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: camera   Connector 2: PC

Value space: Connector 1: camera   Connector 2: 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..2

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: "Camera"   Connector 2: "PC"

Value space: String (0, 50)

- Name for the video input connector.

Video Input Connector [n] OptimalDefinition Profile

n: 1..2

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..2

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: 2..2

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 n: 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: 2..2

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

- 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 n: 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:** 2..2

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.

Requirements: ADMIN, INTEGRATOR

Default value: Connector n: 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:** 2..2

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.

Requirements: 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..2

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

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

Requirements: ADMIN, INTEGRATOR

Default value: Connector 1: Never, Connector 2: Always

Value space: Connector 1: Never, Connector 2: 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 Output Connector [n] CEC Mode

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] Resolution

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..1

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: 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
  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.

- Tap **Call** to make a call, and to invoke the Favorites, Directory and Recents contact lists.
- Tap **Messages** to invoke the voice mail system, if available.
- Tap **Camera** icon to activate self-view and camera control.
- Tap **Share** to start sharing content and to conduct presentations.
- Tap **Microphone** button to mute and unmute microphones.
- Time of day.
- Entry point for user interface extensions (your device may have zero or more such buttons with different color, text and icons).
- Press and hold the left side of the Volume button to decrease the loudspeaker volume and the right side to increase the volume.
- Press the Help desk button to contact the Help desk or access other facility services, if available.
Using Room Kit Mini as a USB camera

The device may be used as a USB camera. This mode makes use of:

- The camera of the device
- The microphones of the device
- The loudspeakers of the device
- If any, the screen that is connected to the device
- A computer with a third-party client

If the device is registered to a call service (cloud or on-premise), you can use the device both as a normal video conferencing device and as a USB camera. The device itself decides which mode it is in. The device is in USB camera mode only when it is streaming media to a computer that is connected to the USB-C port.

If the device is not registered to a call service, you can still use the device as a USB camera.

Set-up and configuration

As an administrator, you don't have to do any special configuration to set up the device as a USB camera.

But you can do some customizations and adaptations for a USB camera only set-up:

- The first time Setup Wizard provides an option of using the device as a USB device only. When choosing this option, you skip the call service (cloud or on-premise) registration.
- Use the UserInterface > WebcamOnlyMode setting to adapt the user interface to a USB camera only scenario when the device is not registered to a call service.

You can choose whether to keep the full user interface on the Touch 10, or to remove elements that are irrelevant when not registered to a call service.

* For example Microsoft Teams, Skype for business, Slack, or Zoom. Cisco successfully tested these clients before product launch. Compatibility between different software versions will not be tested regularly.

Connect to USB-C

To be used as a USB camera, the device must be connected to a computer as shown below, and the connection must be active (the computer cannot be in sleep mode).

You can control the camera and volume from the Touch 10. Other functionality is controlled by the third-party client on your computer.

Use the screen that is connected to the device

USB-C:

- Video and audio from the camera and microphone of the video conferencing device to the computer client
- Audio from computer client to the loudspeakers of the video conferencing device

HDMI-in and HDMI-out:

- Video from the computer client (far end), via the video conferencing device, to the screen

Video resolution

Supported video resolution:

- 720p
- 1080p

Minimum requirements

Minimum USB version:

- USB 2.0

Minimum computer operating system:

- Windows 7
- OS X 10.6
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.

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

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.

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.

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

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.

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.

* When searching, matching entries from the Favorites, Directory and Recents lists will be listed as you type.
Place a call using the web interface (page 2 of 2)

Sign in to the web interface and navigate to Call Control.

Calling more than one

A point-to-point video call (a call involving two parties only) can be expanded to include one more participant on audio-only.

If your 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.

Volume down

Volume up
Share content using the web interface

Sign in to the web interface and navigate to Call Control.

Share content

1. Click Start Presentation. Then the text changes to Stop Presentation.

Stop content sharing:
Click the Stop Presentation button that is present while sharing.

About content sharing

You can connect a presentation source to the video input 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.

* 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.

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.
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 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 best overview is switched on.
1. 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.
2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.
   Only relevant controls appear in the window.
3. Click Close to close the window.

Move the camera to a preset position
1. Click Presets... to open a list of available presets.
   If no presets are defined, the button is disabled and named No presets.
2. Click a preset’s name to move the camera to the preset position.
3. Click Close to close the window.

You cannot use the web interface to define a preset; you should use the Touch controller.
When you select a preset, best overview 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

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

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 GetDetailLevel: Full

The Call History command is available from the API (Application Programming Interface). Refer to the API Reference Guide for your product 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 \( \text{dBA} \), 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

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).

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.

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

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 suit 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 > Call > 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](https://www.cisco.com/go/in-room-control-docs)
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:
```plaintext
*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:
```plaintext
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.
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.

### 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>] [ResultBody: 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.

### 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.

### 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](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.

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:

<table>
<thead>
<tr>
<th>Video conferencing device</th>
<th>Maximum number of different input sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2</td>
<td>2</td>
</tr>
<tr>
<td>Codec Plus, Room 55, Room 55 Dual, Room 70</td>
<td>3</td>
</tr>
<tr>
<td>SX80, MX700, MX800, Codec Pro, Room 70 G2</td>
<td>4</td>
</tr>
<tr>
<td>SX10, DX70, DX80</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

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
```

![Equal Layout Example](image1)

```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP PIPPosition: LowerRight PIPSize: Large
```

![PIP Layout Example](image2)

```
xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: Prominent
```

![Prominent Layout Example](image3)
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:

<table>
<thead>
<tr>
<th>Video conferencing device</th>
<th>Maximum number of different presentation sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room Kit, Room Kit Mini, SX20,  MX200 G2, MX300 G2, Board</td>
<td>2</td>
</tr>
<tr>
<td>Codec Plus, Room 55,</td>
<td>3</td>
</tr>
<tr>
<td>Room 55 Dual, Room 70</td>
<td></td>
</tr>
<tr>
<td>SX80, MX700, MX800, Codec Pro, Room 70 G2</td>
<td>4</td>
</tr>
<tr>
<td>SX10, DX70, DX80</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

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.
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
```

Refer to the API-guide for more details.
Manage startup scripts

Sign in to the web interface and navigate to Integration > Startup Scripts.

List of startup scripts
You can create one or more startup scripts. A green dot appears next to an active startup script; a red ring appears next to an inactive startup script.

If you have more than one startup script, they will run in the order from top to bottom of the list.

Create a startup script
1. Click Create new....
2. Enter a name for the startup script in the title input field.
3. Enter the commands (xConfiguration or xCommand) in the command input area. Start each command on a new line.
4. Click Save.
5. Click On to activate the startup script.

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

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.
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).

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

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.

Power
Always use the provided power supply. The device powers up automatically, as long as the power switch is in its On position.

Maintenance
Micro USB connector for serial communication with the device.

USB
- USB 2.0 type A
- USB 2.0 type C

Monitor output
HDMI version 2.0, resolutions up to 3840 x 2160 at 60fps. There is no audio on the output. You need Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables.

Presentation input
HDMI version 1.4b, resolutions up to 3840 x 2160 at 30fps for computer. You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable.

Network
Ethernet interface, 10Mb / 100Mb / 1Gb Ethernet LAN interface (RJ45).

Touch 10 controller
Touch 10 is powered over Ethernet, which is provided through this socket.
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.

<table>
<thead>
<tr>
<th>Product</th>
<th>Number of auxiliary network ports</th>
<th>Number of auxiliary network ports with PoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room Kit</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Room Kit Mini</td>
<td>1</td>
<td>1 ( )</td>
</tr>
<tr>
<td>Room 55</td>
<td>1</td>
<td>1 ( )</td>
</tr>
<tr>
<td>Room 70 / Room 55 Dual</td>
<td>2</td>
<td>1 ( )</td>
</tr>
<tr>
<td>Room 70 G2</td>
<td>4</td>
<td>2 ( , PoE)</td>
</tr>
<tr>
<td>Codec Plus</td>
<td>2</td>
<td>1 ( )</td>
</tr>
<tr>
<td>Codec Pro</td>
<td>4</td>
<td>2 ( , PoE)</td>
</tr>
<tr>
<td>Boards</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SX10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SX20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SX80</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>MX200 G2 / MX300 G2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>MX700 / MX800</td>
<td>2</td>
<td>0*</td>
</tr>
<tr>
<td>DX70 / DX80</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

* 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.
Serial interface for maintenance

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

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

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

Parameters:
- Baud rate: 115200 bps
- Data bits: 8
- Parity: None
- Stop bit: 1
- 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.

---

1 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.

2 You need a CP210x USB to UART Bridge 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
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 Egde)
- 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
   - xxxxxxxxxxxxxxx

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.
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 (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)
Technical specification (page 1 of 2)

SOFTWARE COMPATIBILITY
- Cisco Collaboration Endpoint Software Version 9.6 or later
- RoomOS

BANDWIDTH
Up to 6 Mbps point-to-point

FIREWALL TRAVERSAL
- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal

VIDEO STANDARDS
- H.264
- H.265 (SIP)

VIDEO INPUT
- One HDMI input*, which supports formats up to maximum 4K (3840 x 2160) at 30 fps, including HD1080p60
- Consumer Electronics Control (CEC) 2.0

VIDEO OUTPUT
- One HDMI output*, which supports formats up to 3840 x 2160 at 60 fps (4Kp60)
- Live video resolutions (encode and decode) up to 1920 x 1080 at 30 fps and 60 fps (HD1080p)
- Consumer Electronics Control (CEC) 2.0

USB PASS-THROUGH
- Ability to provide video, microphone, and speakers over one USB cable to a connected computer
- 720p video resolution

AUDIO FEATURES
- High quality 20kHz audio
- Automatic gain control (AGC)
- Automatic noise reduction
- Active lip synchronization

AUDIO INPUTS
- One audio in from HDMI
- Internal microphones

LOUDSPEAKERS (integrated)
- Three high-quality loudspeakers in balanced configuration
- Frequency response: 70 Hz to 20 kHz
- Amplifier power: 24 W
- Max output level: 85 dB SPL

MULTISITE
- H.239 dual stream (H.323)
- BFCP dual stream (SIP)
- Support for resolutions up to 3840 x 2160 at 5 fps

DUAL STREAM
- One HDMI input supports formats up to maximum 4K (3840 x 2160) at 30 fps, including HD1080p60
- Consumer Electronics Control (CEC) 2.0

WIRELESS SHARING
- Cisco Webex Teams App (up to 3840 x 2160 at 5 fps)
- Cisco Webex Meetings App (up to 3840 x 2160 at 5 fps)
- Cisco Intelligent Proximity client (up to 1920 x 1080 at 5 fps)

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 1080p30 without content. Resolution up to 720p30 and content up to 1080p15
  - Four-way: Resolution up to 720p30 and content up to 1080p15
- 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 x 2160 at 5 fps
- 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)

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
- Media adaptation and resilience
- 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])

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 both static and automatic IP configuration (stateless address auto configuration)

CISCO UNIFIED COMMUNICATIONS MANAGER
- Native registration with Cisco Unified Communications Manager (CUCM)
- Requires CUCM version 9.1.2 or later with device pack for Cisco Webex Room Kit Mini

SECURITY FEATURES
- Management using HTTPS and SSH
- IP administration password
- Administration menu password
- Disable IP services
- Network settings protection
- Privacy cover

NETWORK INTERFACES
- One Ethernet (RJ-45) 10/100/1000 Mbps for LAN
- One Ethernet (RJ-45) for Cisco Touch 10
- Wi-Fi: IEEE 802.11a/b/g/n/ac 2.4 GHz, 5 GHz, 2x2 MIMO

OTHER INTERFACES
- One USB 2.0 port type A
- One USB 2.0 port type C
- One micro USB port
- Factory reset pinhole

OPTIONAL HARDWARE COMPONENTS
- HDMI presentation cable 8 m / 26.2 ft.
- 4 m / 13.1 ft USB cable for USB passthrough feature
- Screen mount kit
Technical specification (page 2 of 2)

CAMERA OVERVIEW
- 4K Ultra HD camera
- Support for up to 60fps (30fps with best overview enabled)
- 8 megapixel image sensor
- 1/1.4 CMOS
- 2x zoom
- f/1.4 aperture
- 120° horizontal field of view
- Automatic framing (face detection)
- Automatic focus, brightness, and white balance
- Focus distance 1 m to infinity

POWER
- 100-240 VAC, 50/60Hz, 12 VDC input
- Average 20W, peak 70W
- Must be used with power supply FSP FSP070-AHAN2 or AcBel ADF019

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)

DIMENSIONS
- Width: 500 mm / 19.7 in.
- Height: 81 mm / 3.2 in.
- Depth: 77 mm / 3 in.
- Weight: 1.8 kg / 4 lbs

APPROVALS AND COMPLIANCE
- Directive 2014/35/EU (Low-Voltage Directive)
- Directive 2014/30/EU (EMC Directive) – Class A
- Directive 2011/65/EU (RoHS)
- Directive 2002/96/EC (WEEE)
- NRTL approved (Product Safety)
- FCC CFR 47 Part 15B (EMC) – Class A
- FCC CFR 47 Part 15C (RF)
- FCC CFR 47 Part 15E (RF)
- FCC Listed (Radio Equipment)

Please check the Product Approval Status Database at http://www.ciscofax.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. 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.
April 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
• RCS1 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco product security overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.bis.doc.gov/policiesandregulations/ear/index.htm.